Escritos presentados por

Javier Smaldone

en la causa

CCC 55276/2019

“NN S/VIOLACIÓN DE CORRESPONDENCIA”

(#LaGorraLeaks 2.0)

Secretaría n.° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n.° 9

Juez: Luis Rodríguez
Fiscal: Ramiro González

#GraciasPatoBullrich

Sr. Juez Federal:

Javier Lorenzo Carlos Smaldone, conjuntamente con mi abogado defensor, Pablo Slonimsqui, en la causa que lleva el nº 55276/2019 del registro de la Secretaría nº 18 de este Juzgado Nacional en lo Criminal y Correccional Federal nº 9, manteniendo el domicilio constituido en el Pasaje Rodolfo Rivarola 193, piso 3º oficina 11 de esta Ciudad Autónoma de Buenos Aires, ante V.S. me presento y digo:

I

Se iniciaron las presentes actuaciones con fecha 30 de julio pasado, cuando la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina puso en conocimiento de la justicia los episodios que conforman el objeto procesal de estos actuados.

Así, conforme se desprende del testimonio de Claudio Ricardo Ramos, Subcomisario con funciones en la dependencia señalada, quien refirió que el 29 de julio pasado se recibió en varias dependencias de la Policía Federal un correo electrónico que simulaba provenir de la Superintendencia de Bienestar, el cual contenía un link que al ser accionado redireccionaría a un formulario el cual solicitaba se completen datos personales y demás información.

Se trata de una maniobra conocida como *Phishing* y permite sustraer datos.

Luego, a través del Ministerio de Seguridad de la Nación, se tomó conocimiento que en la red social Twiter un usuario *@lagorraleaks* refirió haber subido a la "deep web" información relacionada con la Policía Federal, específicamente de las áreas de bienestar y drogas peligrosas, razón por la cual se supone que la información allí publicada puede ser la obtenida a través del mecanismo antes descripto.

La "deep web", se aclara, es un área de Internet sin control por parte de las empresas internacionalmente conocidas, como Google, y donde resulta muy difícil rastrear a los usuarios e información que allí se vuelca.

A partir de las alertas emitidas por la empresa Gmail se pudieron individualizar dos IPs que se corresponderían con las conexiones utilizadas por la persona que habría obtenido los datos de forma engañosa tras ingresar en la cuenta oficial de la Policía Federal sin autorización.

Y, siempre en el concepto del Subcomisario Ramos, teniendo en cuenta la modalidad y tipografía utilizadas por el usuario de Twitter *@lagorraleaks*, se lo puede relacionar con las personas que en el año 2017 hackearon la cuenta de la Ministra Patricia Bullrich.

Sobre esta base, se dio curso a una investigación tendiente a individualizar a los autores del hecho —cuya gravedad no solo nadie discute, sino que yo mismo puse de manifiesto públicamente a través de mi cuenta de Twitter inmediatamente de conocidos los acontecimientos—, investigación que muestra como dato

significativo, de un modo evidente, manifiesto, notorio y ostensible, la intención de vincularme con estos episodios, aun cuando para ello haya que recurrir a métodos que resultan particularmente infantiles.

II

Puede verse de lo actuado que, a la par de una investigación racional, estructurada sobre elementos objetivos de análisis, mediando una creatividad de dimensiones modestísimas se pretende ubicarme como responsable de algo, de cualquier cosa, vinculado con los hechos investigados, aun cuando surge nítido del legajo mi total ajenidad respecto de los mismos.

Y digo así, puesto que habiendo compulsado las actuaciones —por momentos con profundo asombro—, no solo no se advierte qué elemento probatorio podría eventualmente sustentar una imputación en mi contra, sino que tampoco se advierte en concreto —ni en abstracto— cuál sería el hecho que se me imputa.

A fs. 67/68 puede verse un informe remitido al Tribunal por la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina, donde se refieren las medidas de investigación realizadas sobre las máquinas de las dependencias policiales vulneradas, y se da cuenta de los progresos de la investigación estructurados a partir de dicho análisis.

Nada que decir sobre ello.

Pero el problema empieza cuando en dicho informe se anuncia que *teniendo en cuenta la posibilidad de que el autor de la maniobra pueda involucrar mayor cantidad de información y hacerla pública, es que personal nuestro se halla avocado* (sic) *a la observación de fuentes abiertas y redes sociales, detectando ciertos usuarios que habrían replicado la publicación en distintas redes sociales y sistemas de chat con la vulnerabilidad investigada.*

Y sigue el informe:

En otro orden de cosas se destaca que esta División llevó a cabo las investigaciones en torno a los hechos suscitados en el año 2017, relacionado al acceso a la cuenta particular de red social Twitter de la Ministra de Seguridad de la Nación generada con el mismo modus operandi investigado en este caso, teniendo en cuenta la existencia actual del usuario de la red social TWITTER denominado @Lagorraleaks2.0, que no solo hace público los datos obtenidos de las dependencias afectadas de esta Policía Federal, sino que también se atribuye los hechos ocurridos en el año 2017 de la siguiente manera: "En enero del 2017 conseguí acceso a varios correos electrónicos del Ministerio de Seguridad, uno de ellos fue el de la actual ministra de seguridad, Patricia Bullrich, a través del cual tomé su cuenta en twitter. Meses más tarde publiqué los emails de varias fuerzas, que se conoció como "lagorraleaks". Defacee la web del ejército (o fue ISIS?), gendarmería, policía de la ciudad y hackee al diputado tonelli"

Ante esta situación, habiéndose comprobado la autoría de los autores involucrados en el hecho del hackeo a la cuenta de Twitter de la Ministra en el año 2017, y la capacidad técnica que estos presentan para llevar a cabo los presentes hechos, y habiendo encontrado publicaciones donde se adjudican estos al mismo tiempo, se considera a estos como posibles responsables del hecho, tratándose de las siguientes personas:

…

…

Javier Smaldone

Este informe es sencillamente escandaloso por una razón elemental: en ningún momento he sido imputado por la justicia por el hackeo a la cuenta Twitter de la Ministra de la Nación, circunstancia que puede verificarse mediante la compulsa de las actuaciones correspondientes, que llevan el nº 1033/17 del registro del Juzgado Nacional en lo Criminal y Correccional Federal nº 2, Secretaria nº 4. Todo lo contrario, en dicho legajo me presenté espontáneamente, se me recibió declaración testimonial, acompañé toda la información que consideré útil y pertinente para dicha investigación y colaboré con la justicia en todo cuanto estuvo a mi alcance.

Así, tampoco tengo la menor relación con la cuenta *@Lagorraleaks.*

Por tal motivo, en la evidencia que se ha incorporado a este expediente un informe que contiene información objetivamente falsa, y que a la postre permitió que progresara una insólita imputación en mi contra, habré de solicitar que sin perjuicio del trámite de las presentes actuaciones, se extraigan testimonios y se formule la denuncia correspondiente a los fines de investigar las razones que motivaron la presentación referida y la identidad de los ideólogos de tan patética estrategia.

Ello, teniendo en especial consideración que a partir de la incorporación de datos mentirosos en un expediente judicial (la policía se permitió el lujo táctico de inventar cosas) se desarrolló una investigación sobre mi persona —desproporcionada en sí misma, y de una intensidad muy superior a la que se verificó respecto del resto de los imputados— inadmisible en un estado democrático, cuyas verdaderas motivaciones exceden, por mucho, la declamada necesidad de investigar los hechos que integran esta causa.

Siento en el alma hacerle perder el tiempo a V.S. con esta nimiedad, pero yo estoy acostumbrado a respetar la ley y me gustaría que la respetara todo el mundo.

Como veremos, se han intentado múltiples alternativas para incriminarme, ninguna con éxito.

Alguien debería responder por semejante atropello.

Retomando el curso de este legajo, podemos ver que a fs. 93/4 obra nuevamente dicho informe de la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina.

Luego, en el marco de un extenso (e intrascendente a mi respecto) informe se da cuenta que el ciberpatrullaje sobre la cuenta *@mis2centavos* no presenta datos de interés (fs.221) y que se detectó que un grupo creado dentro de la red social Telegram llamado “La gorra Leaks Team” y “Lagorraleaks 2.0”, comparte tweets de *@mis2centavos* en temas relacionados a “las elecciones 19”.

Menciones de mi cuenta cuya vinculación con estos actuados no se alcanza a comprender pueden verse a fs. 224/vta., 225, 225, 227 y 231. Se trata, en lo esencial, de opiniones políticas y conceptos técnicos que interesan a quienes se dedican a la informática.

Llegamos así al informe obrante a fs. 236/43, mediante el cual la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina repasa los antecedentes de su tarea en el caso, y en cuanto aquí interesa señala que:

Por todo lo expuesto, hasta el momento se puede confirmar a prima face (sic) *dos tipos de acciones delictivas hacia las instituciones y funcionarios públicos.*

Uno de los ataques es la realizada a la seguridad informática de la Policía Federal Argentina (en el caso que nos ocupa), Prefectura Naval Argentina y a la Policía de la Ciudad, la cual dejó vulnerable la Seguridad Nacional ante los ciudadanos.

El segundo ataque se realizó con la utilización de las distintas redes sociales, portales públicos, plataformas de la web, etc; publicaciones que no solo dejan al descubierto documentos y/o datos sensibles y privados, sino que fomentan en sus comentarios e instigan a un accionar ciudadano contra las instituciones y funcionarios del Estado Nacional y de las Fuerzas Armadas y de Seguridad.

Es por ello, que el presente hecho delictivo derivó en 2 (dos) líneas principales de investigación: una el seguimiento de los resultados de los datos que arrojaron los servidores vulnerados y la otra línea investigativa sobre el monitoreo/análisis de las publicaciones por el atacante informático, como así también sobre otras publicaciones que puedan relacionarse a las mismas (posteos, comentarios, retwitteos, compartimiento de enlaces, etc).

Expresado el hecho, se observó en las publicaciones del atacante una posible relación con el hackeo efectuado a la Sra. Ministra de Seguridad de la Nación, en el año 2017, en virtud que la intromisión al correo de la Sra. Ministra fue realizada en dicho año por quien se autodenominada "La Gorra Leaks", ilícito investigado por la Policía Federal Argentina, específicamente por la División Delitos Tecnológicos del Departamento CIBERCRIMEN, que era comandado por el Comisario Víctor Chanenko, quienes eran los encargados de la investigación en 2017 y a los que se mencionan despectivamente en las publicaciones que nos ocupan.

Atento a ello, como dato de interés se vinculó a la investigación las personas que posiblemente tuvieron alguna relación con el hecho investigado en el año 2017, procediéndose a realizar búsquedas de publicaciones de los mismos en los distintos portales de fuentes abiertas y/o redes sociales, a fin de poseer algún dato de interés a la causa, siendo las personas a considerar:

…

…

Javier Smaldone (el cual utiliza la cuenta @misdoscentavos) (sic)*. El mismo se presentó en su momento en la causa del año 2017 (hackeo a la Ministra de Seguridad) al enterarse nombrado en las investigaciones. Es muy activo en redes sociales con la temática del voto electrónico y uno de los primeros en publicar sobre las filtraciones que se investigan.*

Siempre en cuanto interesa a esta presentación, señala el informe a mi respecto:

Se obtuvieron las siguientes cuentas @mis2centavos (Twitter), www.facebook.com/javier.smaldone, @javier.smaldone (Instagram) y un @blog.smaldone.com.ar (derivado del Facebook). Cabe señalar que Javier Smaldone en su información consta que vive en Córdoba y que su actividad laboral es programador. Asimismo, posteó en red social a Capitán_Alfa cuando este último refirió haber encontrado vulnerabilidades de un satélite con un amigo.

Hasta aquí, nuevamente información a todas luces intrascendente, y absolutamente nada que me vincule con la investigación que refiere al seguimiento de los resultados de los datos que arrojaron los servidores vulnerados, ni mucho menos con la difusión de los datos ilegalmente obtenidos.

Luego, en el marco de un nuevo informe (fs. 432) puede verse que he sido rigurosamente investigado.

Se dice:

Domicilio: Rivadavia [redacted], Rio Cuarto, Provincia de Córdoba.

Novedades: Se logró detectar movimiento dentro del recinto, observando una silueta masculina mirando por las rendijas de la persiana, motivo el cual se solicita información a la empresa prestataria del Servicio de Internet, diligenciar con la D.N.R.P.A. si posee vehículos a su nombre y la instalación de cámaras de vigilancia (resultado negativo). Asimismo, se informa que el investigado posee dos (2) hijos (que llevan su apellido) con la señora [redacted], quien se domicilia en la calle [redacted], Ciudad de Rio Cuarto. Seguidamente, se hace mención que una de las señales Wi Fi próximas al domicilio investigado, podrían vincularse con el símbolo de los atacantes [S]. Asimismo se pudo determinar mediante tareas desplegadas en el domicilio de Rivadavia [redacted], Rio Cuarto, que el Sr. Smaldone utilizaría un celular con el número 358[redacted] y 358[redacted] (este último de la ex mujer) ambos de la empresa Personal.

Asimismo mediante la utilización de Reporte de geolocalización se logró determinar a través del número 358[redacted] que las antenas lo ubican en inmediaciones del Barrio de Recoleta, Juncal y Montevideo, diligencia practicada el 28/8/2019 horas 15.45, distante 200 metros aproximadamente del domicilio que registrara gretelcamos@gmail.com a través de Mercado Libre, en Av. Santa Fe 1748, CABA, tratándose de un comercio donde no fue habido el buscado ni es conocido, de la misma manera se realizaron nuevas tareas en inmediaciones y contándose con el domicilio de Santa Fe 1635, donde según informe de Mercado Libre fueron entregados los celulares marca XIAOMI, se trata de un edificio de ocho pisos con dos departamentos por cada uno de ellos, donde no fue habido Smaldone ni es conocido; por lo cual y habiendo efectuado una nueva geolocalización la misma dio en [redacted], siendo vista una persona de similares características fisonómicas ingresar al domicilio de dicha arteria en la numeración [redacted], donde las tareas determinaron que allí vive sin poder certificarse que se trate del mismo. Por otro lado, se continuaron tareas en las inmediaciones y con fecha 11 de septiembre del corriente año se visualizó una pareja compuesta por una mujer y un hombre; surgiendo de las tareas en el lugar que se domicilian en la misma arteria pero en la numeración [redacted], piso [redacted] departamento [redacted] CABA, obteniéndose vista fotográfica y casi con exactitud se trataría de Javier Smaldone…

Sobre este informe, puedo decir que:

1.- No advierto de qué modo —la policía tampoco lo explica— una de las señales WiFi próximas a mi domicilio en Río Cuarto podría vincularse con el símbolo de los atacantes [S]. Y tampoco tengo claro —la policía tampoco lo dice— qué podría significar ello a los fines de esta investigación.

2.- Las antenas telefónicas de mi celular me ubican a [redacted] metros del domicilio donde me alojo cuando estoy en esta Ciudad, en una de las zonas más densamente pobladas y con actividad comercial de la misma.

Luego, a fs. 488 luce un pedido de la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina que, por sus características, ya pone de manifiesto sin ambages la intención de avanzar sobre mi intimidad con total independencia de la investigación en curso.

En este escenario, cuando todos los esfuerzos por vincularme con el caso fracasaron estrepitosamente, aparece un informe incalificable.

Puede verse a fs. 515 bajo el título: *Indicios que componen en su conjunto una sospecha fundada bajo los criterios de investigación policial respecto de la vinculación de Javier Smaldone con los hechos investigados.*

El informe está estructurado del siguiente modo:

Análisis previo:

1. En el hecho investigado se ha publicado mediante la red oscura información confidencial de personal policial de la PFA. Dicha información fue obtenida mediante ataques informáticos a sistemas.

Indicios:

1. Indicio: Sindicación por parte de terceros.

2. Indicio: Intereses en común.

3. Indicio: Iniciativa en publicación (concepto de "quema controlada").

4. Indicio: Análisis temporal causa efecto (modo privado de la cuenta).

5. Indicio: Hostigamiento hacia el personal policial que investiga causas conexas.

6. Indicio: Aversión hacia la policía manifestada en forma pública.

7. Indicio: Publicación de análisis de casos investigados.

8. Indicio: Vinculación con actores de causas conexas.

9. Indicio: Análisis de información técnico-informático.

10. Indicio: Análisis de información geo-referencial temporal.

11. Indicio: Información obtenida mediante pedidos de informes.

Consideraciones.

1. Si bien la aclaración es redundante a las reglas de la propia disciplina de la investigación policial, se hace mención que los intereses el uso de herramientas o conocimientos técnicos específicos por si solos no son elementos que generen una sospecha fundada, pero analizados de forma íntegra, en un contexto determinado, con elementos concurrentes y concomitantes producen un cuerpo de análisis que nutre a la investigación y reducen incertidumbres. Es así que los análisis parciales o con falta de integridad respecto de este cuerpo de indicios no componen el presente análisis completo y carecen de integridad.

El informe al cual me vengo refiriendo, plagado de reflexiones primitivas, es desopilante, un maltrato a la inteligencia, por las siguientes razones.

1) Sindicación por parte de terceros.

Aparentemente, un posteo dice: "*Smaldone strikes again (Hackearon a la PFA edition)"* y alguien twiteó "*Che Smaldone, deja de hackear sitios".*

2) Intereses en común.

Se observa intereses en común respecto de la información visualizada en el ataque con el perfil analizado: Voto electrónico, Pablo Tonelli, Patricia Bullrich (¿????). Esto es significa que por criticar de manera pública y particularmente fundada una cuestión de máximo interés para todos los ciudadanos como lo es todo cuanto se vincula con nuestro proceso electoral, tengo un interés común con quien vulnera la seguridad informática de la Policía. Un médico ahí.

3) Iniciativa en publicación (concepto de "quema controlada").

Se visualiza diversas publicaciones donde Javier Smaldone hace referencia a ataques no se adjudica la autoría, pero da difusión de los mismos generando difusión de los daños generados. A la vez también se visualiza publicaciones en medios periodísticos donde da explicaciones de los mismos como "consultor" o "técnico" (¿????). A esto, en los lugares civilizados se lo conoce como periodismo.

4) Análisis temporal causa efecto (modo privado de la cuenta).

En el marco de la investigación y donde se realizando diversas tareas Javier Smaldone bloquea la visualización a su cuenta actual de twitter (@mis2centavos), si bien se refiere a un hecho difundido en medios periodístico (https://www.abcdiario.com.ar/espectaculos/2019/8/26/alfredo-casero-explotó-contra-smaldone-que-panquequeada-pegaste-6984.html) a la vez coincide en los momentos de las tareas propias de la investigación (¿????).

Esta afirmación supone que yo estaba al tanto de los contornos de la presente investigación, y justo —justo— cuando la policía intento visualizar mi cuenta, activé la función de proteger mis tweets. Como si de tal modo pudiese impedir el progreso de la investigación.

5) Hostigamiento hacia el personal policial que investiga causas conexas.

De forma constante y persistente se realizan hostigamientos hacia el personal policial que realizó tareas de investigación manifestando "besis, cabo Landajo" o "Y agarrate, vos, ayudante del cabo Landajo porque te voy a mandar al frente hasta con el color favorito de calzoncillos. Buche de cuarta". Dicho hostigamiento

virtual constante y persistente también, es referenciado en su blog personal (¿????). A todo evento, pongo en conocimiento del Tribunal que, más allá de enfrentar un hecho inédito en materia social, cuál es la policía quejándose de bullying, mantengo una relación pública de tono crítico con dicha fuerza, desde la primera vez que se intentó vincularme con una investigación criminal. La empezaron ellos.

6) Aversión hacia la policía manifestada en forma pública.

De forma constante se manifiesta aversión hacia la policía (¿????).

7) Publicación de análisis de casos investigados.

Se observa como realiza un análisis detallado de diversos casos obteniendo información de terceras partes (¿????). Nuevamente, en los lugares civilizados a esto se le llama periodismo.

8) Vinculación con actores de causas conexas.

Se observan vinculaciones entre la cuenta analizada y otras cuentas como LIberoamericaMU, Capitan_Alfa, Hispahak (¿????). Solo diré aquí que en mis más de nueve años de uso de la red social Twitter, con cierto protagonismo en mi esfera de conocimiento y habiendo llegado a tener más de treinta y seis mil seguidores, mantuve "vinculaciones" con muchísimos usuarios cuya actividad privada ciertamente desconozco.

9) Análisis de información técnico-informático.

En los ataques se visualiza información técnica concordante con las descriptas por el actor tanto en la cuenta de Twitter como así en su CV (¿????). Se sugiere aquí que por mis conocimientos, me encuentro en condiciones de llevar adelante la maniobra investigada. Yo —y olvidó la policía decir— miles de personas más, solo en nuestro país, que se interesan por la informática.

10) Análisis de información geo-referencial temporal.

Respecto de la información geo-referencial se aprecia lo siguiente: i) misma ubicación entre Emanuel Velez Cheratto y Javier Smaldone son de la Provincia de Córdoba, ii) Javier Smaldone realiza una visita a Santa Fe específicamente en la localidad de Santo Tomé, donde hay vinculaciones con diversas acciones en la referente causa (donde fue como observador electoral colaborando con la Fundación Poder Ciudadano, capitulo argentino de Transparency International). Dicha visita, se omite aclara, ocurrió en el mes de abril de este año, *iii) la contratación de Fulltech (Santa Fe 1748) se declara en un domicilio cercano a la ubicación real de Javier Smaldone y iiii) Celulares XIAOMI se generan compras con domicilio de envío en Santa Fe 1635, ubicación cercana a la ubicación real de Javier Smaldone, según información provista por Mercado Libre.*

11) Información obtenida mediante pedidos de informes.

Según información analizada de los pedidos de informe a las empresas de telefonía celular, se observan similitudes respecto de los momentos de alta del VPS y solicitud de baja. Viendo que ambos cuentan con patrones similares de la señal de telefonía celular (¿????). Incomprensible.

Este informe muestra, en mi modo de ver las cosas, que la especie humana, tras siglos de civilización, sigue conservando rasgos barbaros: en franco desconocimiento del arte de la fundamentación, la línea que separa lo real de lo imaginario aparece aquí un tanto difusa. Basta tener estudios elementales para advertir que mediante este informe se fuerzan, hasta el absurdo, argumentaciones carentes de todo sustento con el único fin de involucrarme en el caso. Un método que se utilizaba hace muchos años para canalizar escarmientos.

En ausencia de un mínimo de consistencia intelectual, con estos métodos de investigación, no me sorprende que una investigación naufrague; me sorprende que llegue a puerto.

¿Para esto pagamos tantos impuestos?

Como en muchos informes policiales, lo de menos es lo que dice; lo único que tiene interés es lo que deja afuera: en el caso, el malestar que genera en ciertos ámbitos políticos mis investigaciones vinculadas con el voto electrónico.

Vuestra Señoría no tiene porqué saberlo, pero desde hace más de veinte años participo públicamente, de manera activa, en distintos debates referidos a cuestiones de máximo interés público. En este último tiempo, he tenido —dicho modestamente— una participación relevante en todo cuanto se vincula al sistema electoral, más concretamente a la introducción de herramientas informáticas en los procesos de votación y escrutinio, con fuertes críticas a la iniciativa del actual gobierno para la implementación del voto electrónico.

Por estas cuestiones expuse ante el plenario de comisiones de la Honorable Cámara de Diputados y dos veces ante el plenario de comisiones del Senado de la Nación.

Ello, además de haber publicado decenas de notas en diferentes medios de comunicación.

Con base en este informe, con fecha 25 de setiembre pasado, la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina solicita de V.S. distintos procedimientos, entre ellos el allanamiento de un domicilio que frecuento, con el objeto de secuestrar telefonía celular, elementos informáticos, dispositivos de almacenamiento, anotaciones y registros vinculados a la maniobra investigada (fs. 533).

III

Sobre la base de estos antecedentes, con fecha 3 de octubre pasado (fs.591) V.S. dispuso el allanamiento que aquí se cuestiona.

Como ha quedado acabadamente descripto, ni mediando un esfuerzo de imaginación superlativo puede sostenerse que existiese a mi respecto, a los fines de disponer una orden de allanamiento en el domicilio donde me alojo cuando visito esta Ciudad, motivos, razones o fundamentos que surjan *legítimamente* ni del propio decisorio que aquí se cuestiona, ni de otra pieza procesal a la cual dicho auto remita en forma inequívoca, ni de constancia alguna arrimada al proceso con anterioridad al dictado del mismo, de la cual surja de forma indudable la necesidad de proceder.

En modo alguno puede siquiera sugerirse que una medida intrusiva de las características de la que aquí nos ocupa sea una derivación lógica de lo actuado hasta el momento, ni una consecuencia categórica de probanzas colectadas con antelación.

No se puede individualizar en todo el legajo un elemento que autorice lo dispuesto por el Tribunal. Así, la lectura de todo lo actuado no permite tener a la vista las motivaciones de la medida dispuesta, violatoria de disposiciones constitucionales que hacen a la protección de mi domicilio y de mi intimidad.

No puedo pasar por alto que so pretexto de desarrollar una investigación que versa sobre cuestiones tecnológicas, se intentó obtener los datos correspondientes a mi tarjeta SUBE y a mi cuenta de *Whatsapp*, a la vez que se colocaron cámaras de vigilancia frente a la vivienda de mis hijos, aun en el conocimiento que yo no me encontraba en el lugar.

Y que estas medidas solo se instrumentaron a mi respecto: el resto de las personas involucradas en esta investigación tuvo mejor suerte.

Para disponer un allanamiento, el auto que lo ordena debe sustentarse en una base seria y suficiente para justificarlo. No basta el cúmulo de información **falsa, tergiversada** e **intrascendente** mediante la cual la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina llevó a engaño al Tribunal, formando su convicción acerca de la existencia de motivos legalmente válidos para fundar su proceder.

Por tal motivo, habré de solicitar se declare la nulidad del auto que ordena el allanamiento cuestionado, y en virtud lo normado en el artículo 172 del Código Procesal Penal de la Nación, la nulidad de todos los actos consecutivos que de él dependen, concretamente, el secuestro verificado en la ocasión.

IV

Y en la misma dirección, habré de postular el dictado de un sobreseimiento a mi respecto, en la inteligencia que no existe el menor indicio (más allá de la imaginación policial) que sugiera que he participado en la intrusión investigada, o en la difusión de la información así obtenida.

Las maniobras investigadas conllevan el peligro a la seguridad nacional que implica que información propia de las fuerzas de seguridad se encuentre en manos de particulares, que podrían afectar intereses de la República Argentina a partir de la revelación de secretos propios de la Policía Federal Argentina.

Por tal motivo, no debe V.S. permitir que se desvíe el curso de la investigación correspondiente, con la evidente intención de vincular al proceso a personas que ninguna relación guardan con el mismo, y al amparo de una supuesta investigación dar amparo a seguimientos inadmisibles en el marco de un Estado de Derecho.

V

En razón de lo expuesto, de V.S. solicito:

1 Se forme incidente de estilo, y oportunamente se declare la nulidad del allanamiento dispuesto sobre mi domicilio, y demás actos procesales consecuentes.

2 Oportunamente, se dicte sobreseimiento a mi respecto, en la inteligencia que no existe elemento alguno que sugiera mi participación en los hechos investigados.

3 Se ordene la correspondiente extracción de testimonios a los fines de investigar los ilícitos mencionados en este escrito.

Tener presente lo expuesto,

SERA JUSTICIA

Nota aclaratoria: respecto del texto presentado en sede judicial se han realizado correcciones de errores de tipeo y de estilo, y se han tachado datos sensibles, para evitar revictimizar a los damnificados.

#GraciasPatoBullrich

Sr. Juez Federal:

Javier Lorenzo Carlos Smaldone, conjuntamente con mi abogado defensor, Pablo Slonimsqui, en la causa que lleva el nº 55276/2019 del registro de la Secretaría nº 18 de este Juzgado Nacional en lo Criminal y Correccional Federal nº 9, manteniendo el domicilio constituido en el Pasaje Rodolfo Rivarola 193, piso 3º oficina 11 de esta Ciudad Autónoma de Buenos Aires, ante V.S. me presento y digo:

I

Que vengo por intermedio de este escrito a acompañar a este legajo, ampliando la presentación hecha días pasados, copia simple de la declaración testimonial que prestara con fecha 16 de mayo de 2017 en el marco de las actuaciones que llevan el n° 1033/17 del registro de la Secretaria n° 4 del Juzgado Nacional en lo Criminal y Correccional Federal n° 2.

De este modo se acredita, sin más, la mentira invocada por el personal policial que interviene en autos a los fines de involucrarme, insólitamente, como sospechoso en esta investigación.

Recuerde V.S. que a tal fin, la policía señaló que yo había sido uno de los autores de los hechos que se investigaron en las actuaciones señaladas, cuando resulta evidente que fui escuchado como testigo.

Y de la simple lectura de la declaración que acompaño se desprende que en la ocasión informé públicamente acerca de los hechos que interesaban a dicho expediente (hackeo a cuentas de correo del Ministerio de Seguridad de la Nación y de la Policía Federal Argentina) así como advertí sobre su gravedad.

Y que colaboré con la justicia en todo cuanto estuvo a mi alcance.

II

Adjunto también a esta presentación una nota escrita en mi blog personal el día 9 de marzo de 2017, en oportunidad de tomar conocimiento de la investigación supra señalada, informando públicamente la realidad de los hechos detectados (en ese momento negados por las autoridades), poniendo de resalto su gravedad.

A la vez, adjunto los tweets publicados por mi el día 12 de agosto de 2019, respecto de la filtración de datos de la Policía Federal Argentina que son mencionados en los distintos informes policiales como motivo de sospecha, y cuyo contenido completo nunca fue puesto en conocimiento de V.S.

La lectura de dichos tweets permitirá al Tribunal analizar lo actuado por el personal policial en el caso desde la perspectiva correcta, y resolver en consecuencia.

III

Soy periodista. Trabajo como programador y administrador de sistemas, pero durante los últimos años he sido autor o colaborador de distintas investigaciones periodísticas. Las más notorias tienen que ver con la empresa Smartmatic (actualmente encargada del escrutinio provisorio en las elecciones argentinas) [1], el sistema de voto electrónico usado en las elecciones de la Ciudad Autónoma de Buenos Aires en 2015 [2], el proyecto de ley para el uso de voto electrónico a nivel nacional impulsado por el Gobierno en 2016 [3] y el descubrimiento de que las computadoras de voto electrónico utilizadas en las elecciones del Congo de 2017 habían sido diseñadas y construidas para su uso en la Argentina [4].

Otras nunca han sido publicadas y algunas —que no puedo mencionar públicamente aún— se encuentran actualmente en curso. En algunas de estas investigaciones he participado de forma *ad honorem*, en otras he sido remunerado.

Por este motivo, casi diario y durante los últimos años, mantengo contacto con periodistas de diversos medios (gráficos, radiales, televisivos y online) y también con fuentes particulares, con quienes intercambio información sensible respecto de investigaciones periodísticas.

No sólo actúo como fuente de periodistas, recibo información de estos y otros, a fin de colaborar en la investigación y la elaboración de las notas. La mayoría de esas conversaciones están en los dispositivos que me fueron secuestrados en el allanamiento ordenado por V.S.

A raíz de una de estas investigaciones, por ejemplo, fui contactado en el año 2018 por el grupo de investigación estadounidense The Sentry, integrándome al equipo que participó del análisis de diversas piezas de información (incluyendo documentos confidenciales filtrados) que permitieron descubrir que las máquinas de voto electrónico que el cuasi-dictador de la República Democrática del Congo planeaba usar para las elecciones —y posiblemente para cometer fraude— en realidad habían sido diseñadas para su uso en la Argentina, donde ni siquiera se había aprobado una ley al respecto, ni mucho menos se había realizado un proceso de licitación [5]. Dicha investigación fue reproducida por medios como Associated Press [6] y The Washington Post [7], como así también en varios medios argentinos. Parte de esa información sensible —cuya divulgación podría poner en riesgo la vida de las personas involucradas en la filtración— se encuentra también en mis computadoras.

En este momento se lleva adelante en la Argentina un proceso electoral que determinará el próximo Presidente de la Nación y la conformación del Congreso. En el marco de dicho proceso, como es público y notorio, me encuentro desde hace tiempo abocado a la investigación de las particularidades y las vulnerabilidades del sistema de escrutinio utilizado.

He informado vulnerabilidades existentes en el mismo [8], en tanto que me encuentro investigando otros posibles riesgos. A raíz del secuestro de mis herramientas, no sólo me he visto imposibilitado de continuar con esta tarea, sino que temo por la integridad y la seguridad de la información contenida en mis dispositivos de almacenamiento.

Por último, le hago saber que incluso en mi cuenta de Twitter y en mi blog personal, ambos espacios virtuales que fueron "ciberpatrullados" por las fuerzas de seguridad, actúo como divulgador y comunicador de hechos (en lo referido a mi área de conocimiento), en una tarea también asimilable al periodismo y por ende bajo el paraguas de la libertad de prensa.

De hecho, en esta tarea es que en el año 2017 —presumiendo una grave filtración de datos sensibles de las fuerzas policiales y ante la falta de información en los medios masivos y la falsedad de las declaraciones de funcionarios gubernamentales— fue que me involucré en la investigación de los hechos relacionados con el "hackeo" a la Ministra Bullrich, el Ministerio de Seguridad y la Policía Federal [9], siendo esto lo que generó la rispidez con esta fuerza y sumó al desagrado de la Ministra Patricia Bullrich hacia mi persona.

Y ahora, en la necesidad de reforzar su autoestima, pretenden ubicarme como responsable de algo, echando mano a recursos que la administración de justicia no puede tolerar. Por lo menos, en los lugares civilizados.

Tener presente lo expuesto,

SERA JUSTICIA

[1] "Smartmatic, la polémica empresa de cómputos electorales que vino de Venezuela a Argentina", Border Periodismo, 7 de agosto de 2017. https://borderperiodismo.com/2017/08/07/masticar-la-polemica-empresa-de-computos-electorales-que-vino-de-venezuela-a-argentina/

[2] "Boleta Electrónica: expertos muestran cómo vulneran el secreto del voto", La Nación, 21 de octubre de 2016. https://www.lanacion.com.ar/politica/la-boleta-unica-electronica-implica-riesgos-para-el-secreto-del-voto-nid1948796

[3] "Voto electrónico. Una solución en busca de problemas", capítulo 1.3. ISBN 9789873789243, marzo de 2017.

[4] "Boleta única electrónica, invento argentino que debuta en la cuestionada democracia del Congo", Border Periodismo, 23 de abril de 2018. https://borderperiodismo.com/2018/04/23/la-boleta-unica-electronica-un-invento-argentino-que-debuta-en-la-dictadura-del-congo/ "Las pruebas de que las máquinas de voto electrónico del Congo se diseñaron para Argentina", Border Periodismo, 28 de junio de 2018. https://borderperiodismo.com/2018/06/28/las-pruebas-de-que-las-maquinas-de-votoelectronico-del-congo-fueron-disenadas-para-usarse-en-argentina/

[5] "Electronic Voting Technology DRC: Security Vulnerabilities and Déjà Vu", The Sentry Team, junio de 2018. https://cdn.thesentry.org/wp-content/uploads/2018/06/DRCelections_SentryAlert_June2018_0619.pdf

[6] "Voting machines raise worries in Congo ahead of elections", Associated Press, 21 de junio de 2018. https://apnews.com/1764856db1b74c7790a05a65d7a9c5b0

[7] "The Cybersecurity 202: The U.S. is warning Congo that using electronic voting machines could backfire", The Washington Post, 10 de septiembre de 2018. https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/10/the-cybersecurity-202-the-u-s-is-warning-congo-that-using-electronic-voting-machines-could-backfire/5b953d2f1b326b47ec9594d2/

[8] "Elecciones 2019: Advertencia de vulnerabilidades críticas en el sistema de escrutinio provisorio", Fundación Vía Libre, 3 de agosto de 2019. https://www.vialibre.org.ar/2019/08/03/elecciones-2019-reporte-de-vulnerabilidades-criticas-en-el-sistema-de-escrutinio-provisorio/

[9] "Patricia Bullrich y el «ciberpatrullaje»", 9 de marzo de 2017. https://blog.smaldone.com.ar/2017/03/09/patricia-bullrich-y-el-ciberpatrullaje/

SEBASTIAN R. RAMOS
JUEZ FEDERAL

Poder Judicial de la Nación

CFP 1033/2017

///n la Ciudad Autónoma de Buenos Aires, a los 16 días de mayo de 2017, comparece ante S.Sa. y Secretaria Actuante, una persona previamente citada a la que se le va a recibir declaración testimonial de conformidad con lo normado por los artículos 249 y 118 del Código Procesal Penal de la Nación. En este estado de cosas se la instruye sobre las penas correspondientes al delito de falso testimonio, leyéndosele las pertinentes disposiciones legales, e invitada que fuera a prestar juramento por sus creencias, expresó: *"JURO DECIR LA VERDAD"*, prometiendo decir verdad en cuanto supiera y le fuera preguntado. Preguntado que fuera por sus datos, dijo ser y llamarse: Javier Lorenzo Carlos Smaldone, quien acredita su identidad con el DNI n°23[redacted] de nacionalidad argentina, nacido el [redacted] en Río Cuarto, Provincia de Córdoba, hijo de [redacted] y [redacted] de estado civil [redacted], de ocupación programador informático, domiciliado en [redacted] Río Cuarto, Provincia de Córdoba; sabe leer y escribir.----------

Preguntado para que diga si le comprenden las generales de la ley –que en este acto se le explican–, respondió: *"No me comprenden"*.------

Preguntado por S.S. para que diga si conoce a los usuarios de la red social *"Twitter"*, *"@OcsinoDeJuliFox"* y *"@LIberoamericaMu"*, y en su caso, dé razón de sus dichos, contestó: *"Las cuentas las he visto, he interactuado con ellos, pero no sé quién o quiénes están detrás de esas cuentas. Digo quienes porque no sé si son más de una persona"*.----------

Preguntado por S.S. para que diga si conoce al usuario de la red socia *"Twitter"* *"@theniggy202"* –Mohammed Hassan–, y en su caso, dé razón de sus dichos, respondió: *"Misma situación, no sé quién, ni quiénes usan esa cuenta. Igualmente, esa cuenta no existe más, hoy lo verifiqué a la mañana"*.----------

Exhibidas las fojas 1805/8 y 1825, y preguntado por S.S. para que diga si ratifica el contenido de las conversaciones y precise las circunstancias de tiempo, modo y lugar, en la que se sucedieron, contestó: *"Ratifico el contenido de las conversaciones. Este usuario me contactó el día 30 de abril de este año, para hacerme llegar un diseño de una página web que yo había pedido ayuda públicamente en Twitter. Yo pedí ayuda en Twitter sobre el diseño visual para una herramienta que yo había desarrollado y este usuario, pasadas unas horas, me envió un mensaje directo por la misma red social, donde me hacía llegar un diseño. Le agradecí, no le pregunté ni quién era ni nada. Ese fue el primer contacto. El segundo contacto fue el 3 de mayo a las 22:32 horas. Esto lo verifiqué con las notificaciones de mi mail. Esto ocurrió inmediatamente después de que yo emitiera una seria de twits, hablando sobre el tema del hackeo a las cuentas del Ministerio de Seguridad. Yo publiqué media hora sobre el tema y acto seguido el usuario me manda un mensaje directo diciéndome textualmente «Te interesan?» y me adjuntó lo que parece ser la captura de pantalla de la bandeja de entrada de la cuenta crimenorganizado@policiafederal.gov.ar. Precisamente en la foja 1805 me pasa un archivo para bajar el diseño y luego el 3 de mayo me adjunta esa captura y ahí se lee «Te interesan?»-No le pregunté ni quién era, ni cómo había sacado eso, sino solamente, le dije que si lo que él quería era poner de manifiesto la endeble seguridad de los sistemas de las fuerzas de seguridad, acudiera a la prensa y les diera información que los periodistas pudieran corroborar. Concretamente, le recomendé hablar con el periodista Julio López, y el me respondió que ya estaba en contacto con el periodista. A Julio López lo conozco previamente por otros trabajos que él hizo, es un informático y periodística, y siento un gran respeto profesional. Desde los primeros sucesos del día 26 de enero, me mantuve en contacto con él, vía telefónica, por mail, etc. Él fue el primero y el único que informó que los eventos del 26 de enero no se limitaban a la cuenta de la ministra*

Bullrich, sino que había sistemas del Ministerio de Seguridad que estaban afectados, en particular la cuenta denuncias@minseg.gob.ar. Por este motivo, siempre recomendé tanto a @LIberoamericaMu, como a @theniggy202 que se comunicaran con él y le proveyeran evidencia que le permitiera verificar por sus propios medios, la violación de la seguridad. Yo luego de esto, de la conversación por mensaje directo, hablé con Julio López, le comenté lo sucedido, le describí lo que había recibido, sin enviarle la captura, y Julio me refirió que el fin de semana anterior había recibido mails de quien decía ser el autor de los hackeos a Bullrich y al Ministerio de Seguridad. Quiero aclarar que en mi conversación con este usuario, luego de enviarme la captura de la bandeja, que no sé si era cierto o no, me dijo que era había sido el autor de los hackeos y se identificó como [S]. Acto seguido, lo llamé a mi abogado y el Dr. Iglesias me dijo que presentara esto que fue lo que sucedió el día después. El 4 de mayo al mediodía a las 12:01 horas, recibí un mail del remitente Nelson.Castro@protonmail.com ("Nelson Alberto Castro") con supuestamente el usuario y contraseña de la cuenta de crimen organizado de la Policía Federal Argentina, lo que no verifiqué, y un enlace para descargar un archivo ZIP con su correspondiente contraseña. Procedí a descargar el archivo, a descomprimirlo y obtuve más de 40 megabytes de archivos PDF., DOCX, XLSX, MP3 y JPG, entre otros, y al examinar un par de ellos, vi que se trataban por ejemplo de órdenes de seguimiento de criminales en donde figuraban los nombres de los mismos y de los policías que debían seguirlos, ante lo cual no quise seguir viendo. Inmediatamente, llamé por teléfono al señor Julio López y ante mi pedido que revisara el mail, me contestó si a mí también me había llegado. Verificamos que se tratara del mismo contenido del mail, y era lo mismo. Lo próximo que hice fue llamar al Dr. Iglesias y el me dijo que le mandara todo lo que había recibido tal cual me había llegado, para presentarlo en la causa. Eso es lo que hice. Luego borré mi copia local de mi disco duro, ya no esta en mi

poder. Quiero aclarar que el día 11 de mayo a las 21:45 horas, el programa TN Central emitió un informe en el que decía que habían sido violadas otras cuentas de correo de las fuerzas de seguridad y del que participó Julio López en el informe periodístico. Al otro día, 12 de mayo a las 11:29 horas, recibí un mail de la cuenta Bohuslav.busek@protonmail.com diciéndome textual "hiciste una denuncia por lo que te envié?, sos un pelotudo". No sé si es el mismo que me mandó la información, no puedo decir que sea el mismo, parece".----------

Preguntado por S.S. para que diga como se contactó y/o contacta con dicho usuario, contestó: *"Por red social Twitter los primeros contactos. Yo el Twitter tengo más de 35.000 seguidores, por lo cual tengo cierta notoriedad. Además, tengo los mensajes directos abiertos, con lo cual cualquier usuario puede mandarme mensajes en privado sin necesidad de que yo lo siga o autorice. No es que yo seguía a este usuario u otros, cualquiera me puede escribir. Además, mi mail es bastante público, se encuentra googleando, con lo cual cualquier persona me puede mandar fácilmente un mail".*----------

Preguntado por S.S. para que diga si tiene forma de identificar al usuario, respondió: *"No".*----------

Preguntado por S.S. para que diga si quiere agregar o enmendar algo de la presente declaración, manifestó: *"Si. La razón por la cual he seguido con bastante detalle los sucesos relacionados con este tema, es que me preocupa la posibilidad de que las cuentas de correo sensibles de las fuerzas de seguridad puedan ser fácilmente accesibles. La evidencia publicada en Twitter y lo informado por medios periodísticos muestran que fueron vulneradas cuentas de correo del Ministerio de Seguridad y la respuesta oficial de sus funcionarios ha sido negar esa situación. Por esta razón, a toda persona que me hizo llegar algún tipo de comentario sobre el tema, a través de mensajes directos de Twitter, le recomendé hablar con la prensa. Hay una cosa más, es otra cosa que yo veo atrás de esto que*

también me preocupa, y que me ha animado a mantener el contacto con estos usuarios de Twitter, es que no veo en ellos la intención de lucrar o causar daño, cosa que podrían haber hecho vendiendo el acceso o publicando el contenido de las cuentas comprometidas, sino la de poner de manifiesto una situación altamente peligrosa para las investigaciones realizadas por las fuerzas de seguridad".----------

Con lo que no siendo para más se dá por finalizado el acto, firmando el compareciente, previa lectura y ratificación de la presente, después de S.Sa. y por ante mí. Doy fe.

SEBASTIAN R. RAMOS
JUEZ FEDERAL

SECRETARIA
Nº 4

ESTEBAN MURANO
SECRETARIO FEDERAL

Patricia Bullrich y el «ciberpatrullaje»

blog.smaldone.com.ar/2017/03/09/patricia-bullrich-y-el-ciberpatrullaje

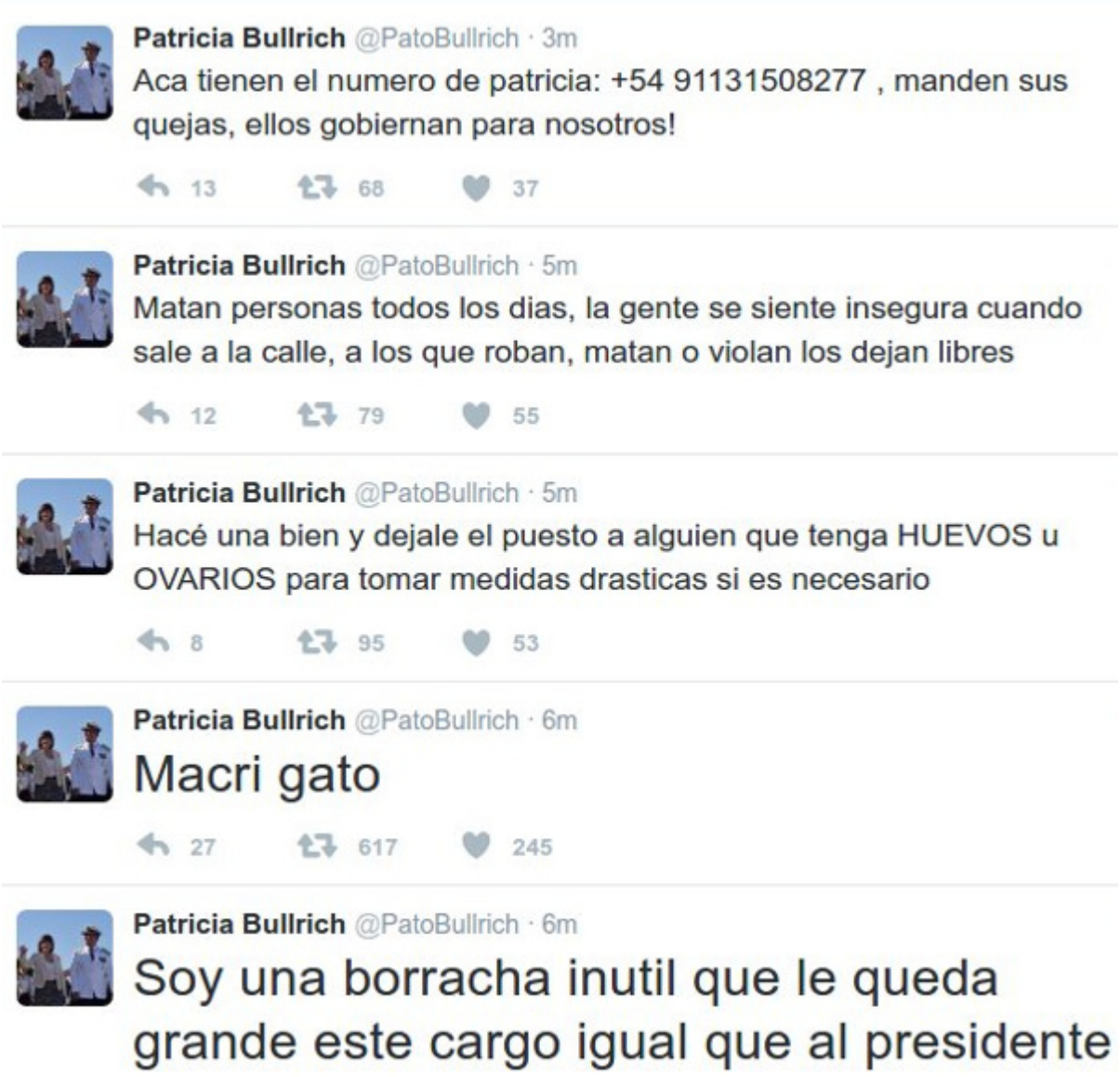
Javier

El 26 de enero de 2017 a la ministra de Seguridad **Patricia Bullrich** le «hackearon» su cuenta de Twitter. Horas después, apareció evidencia de que el problema era más grave e involucraba a varias cuentas de correo del **Ministerio de Seguridad**. Un mes después fueron detenidas dos personas acusadas del hecho.

Con gran sorpresa, ayer me encuentro con que aparezco nombrado en la causa penal. Y, peor aún, que he sido investigado. A continuación, el relato de lo que pasó.

El «hackeo»

Estos son los tweets que aparecieron en la cuenta de **Patricia Bullrich**:



Pasó más de una hora sin que nadie los borrara, mientras la ministra estaba en un acto oficial del Ejército. Afortunadamente, tomé el recaudo de guardarlos en archive.org.

Hasta ahí, parecía que el problema se reducía a que alguien había logrado tomar control de la cuenta de Twitter de **Bullrich**. Pero unas horas más tarde, empezaron a aparecer capturas de la «bandeja de entrada» de varias cuentas del **Ministerio de Seguridad** (incluyendo la de la ministra).

> **#NOalVotoElectrónico #BoletaÚnicaPapelYA**
> @mis2centavos2
>
> Hum... parece que la cuenta de @PatoBullrich no fue lo único que hackearon en el @MinSeg. Aprecien: twitter.com/LIberoamericaM…
>
> 8 19:42 - 26 ene. 2017
>
> Ver los otros Tweets de #NOalVotoElectrónico #BoletaÚnicaPapelYA

> Ministerio de SEGURIDAD. Un chiste, como @PatoBullrich.https://t.co/dy2WSesal4
>
> — Javier Smaldone (@mis2centavos)

#NOalVotoElectrónico #BoletaÚnicaPapelYA
@mis2centavos2

A @PatoBullrich le mandaron un email "Entrá acá usando tu cuenta de #Twitter y te regalamos un vino". Y entró. twitter.com/LIberoamericaM…

57 19:58 - 26 ene. 2017

31 personas están hablando de esto

Como puede apreciarse, los tweets adjuntos a cada uno de los míos fueron eliminados. Afortunadamente, también tuve el recaudo de descargar las imágenes que incluían y volver a tuitearlas.

#NOalVotoElectrónico #BoletaÚnicaPapelYA
@mis2centavos2

Mandás un email a denuncias@minseg.gob.ar para denunciar narcos. Los narcos lo leen, van a tu casa y te cagan a tiros. Bien, @PatoBullrich.

140 19:54 - 26 ene. 2017

145 personas están hablando de esto

#NOalVotoElectrónico #BoletaÚnicaPapelYA
@mis2centavos2

CONFIRMADO: Cuentas de email del @MinSeg vulneradas (incluyendo la que recibe las denuncias). No fue sólo el Twitter de @PatoBullrich.

135 8:46 PM - Jan 27, 2017

235 people are talking about this

Desde la misma cuenta de Twitter que se habían publicado las capturas anteriores, se dieron más detalles sobre el «hackeo»:

Libero
@LIberoamericaMu

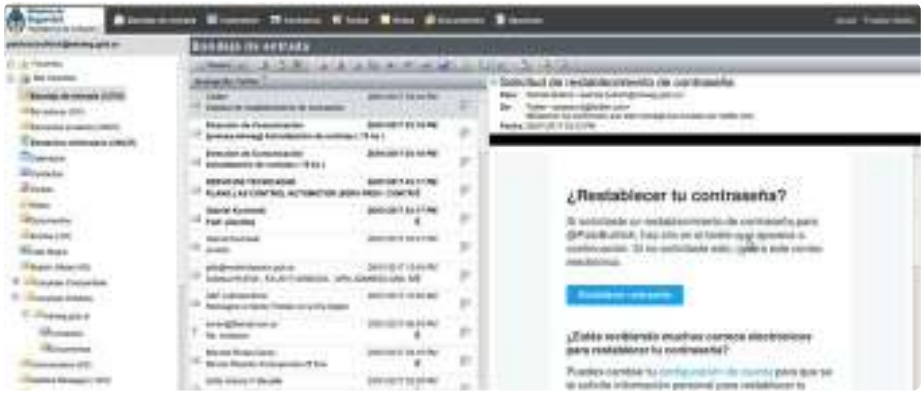
jajaja miren como hackearon a la ministra, le mandan un mail haciendose pasar por embajador y redireccionaron un link al scam de twitter

360 20:58 - 26 ene. 2017

294 personas están hablando de esto

Libero
@LIberoamericaMu

Momentos antes de resetear la password a la ministra :p



89 20:59 - 26 ene. 2017

85 personas están hablando de esto

(Aquí puede ver la captura del primer tweet y la captura del segundo tweet, por si son eliminados).

Luego, desde otras cuentas de Twitter empezaron publicarse capturas de pantalla y volcados de bases de datos, algunos de varios meses antes, que parecían provenir del **Sistema Nacional de Información Criminal** (SNIC). Finalmente, un usuario identificado como «*Niño Orsino*» (cuya cuenta de Twitter luego desapareció), comenzó a auto-adjudicarse la violación de las cuentas del **Ministerio de Seguridad** y del Twitter de **Bullrich** y luego hasta dio una nota a un medio periodístico. Esta persona resultaría ser más adelante una de las dos imputadas y detenidas, después la única procesada (hasta el momento).

Nota: Por lo que puede verse, y luego confirmaría el auto de procesamiento, ***Bullrich*** *usaba su dirección de email oficial en el* ***Ministerio de Seguridad*** *para su cuenta personal de* ***Twitter****. Fue víctima de un «phishing», mediante el cual el atacante logró obtener el usuario y la contraseña de su cuenta de email, y luego accediendo a esta pudo cambiar su contraseña en la red social.*

La mentira de Bullrich

En un primer momento, **Bullrich** reconoció el «hackeo» de su Twitter. Luego, a pesar de que todos los indicios mostraban que el problema era bastante más grave de lo que parecía al principio, desde el **Ministerio de Seguridad** afirmaban que no había cuentas de email comprometidas. Claramente estaban mintiendo, y esto fue advertido por el periodista Julio López:

#NOalVotoElectrónico #BoletaÚnicaPapelYA · 27 ene. 2017
Insisto: vean esto, aunque no se entienda todo. Habrá más novedades.twitter.com/i/moments/8247…

El hackeo a @PatoBullrich y al @MinSeg

#NOalVotoElectr… @mis2…

Hackearon la cuenta de Twitter de

Moments

#NOalVotoElectrónico #BoletaÚnicaPapelYA
@mis2centavos2

Acá @julitolopez comenta lo que sospechábamos ayer: "hackearon" cuentas de correo electrónico de @MinSeg. Hola, @PatoBullrich.

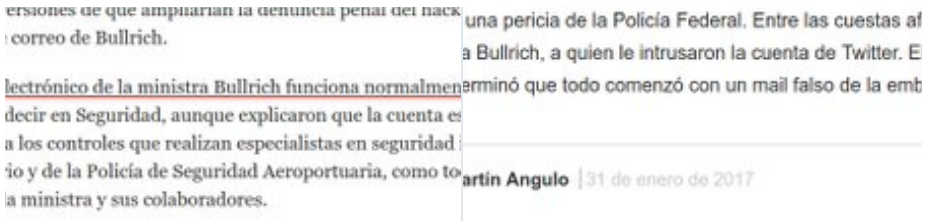
29 19:11 - 27 ene. 2017

29 personas están hablando de esto

También, tímidamente, el diario **La Nación** se animaba a deslizar que había cuentas oficiales del **Ministerio de Seguridad** involucradas en el incidente (lo que ya para el 28 de enero estaba completamente confirmado). Finalmente, se comprobó: múltiples cuentas de email habían sido comprometidas (40, exageraba el diario **Clarín**).

#NOalVotoElectrónico #BoletaÚnicaPapelYA
@mis2centavos2

El @MinSeg y @PatoBullrich mintieron para ocultar el "hackeo": las capturas eran auténticas, y ellos lo sabían (podían comprobarlo).


ersiones de que ampliarían la denuncia penal del hack
correo de Bullrich.

lectrónico de la ministra Bullrich funciona normalmen
decir en Seguridad, aunque explicaron que la cuenta es
a los controles que realizan especialistas en seguridad
io y de la Policía de Seguridad Aeroportuaria, como to
a ministra y sus colaboradores.

una pericia de la Policía Federal. Entre las cuestas af
a Bullrich, a quien le intrusaron la cuenta de Twitter. E
erminó que todo comenzó con un mail falso de la emb

artín Angulo | 31 de enero de 2017

35 14:04 - 31 ene. 2017

35 personas están hablando de esto

Las detenciones

Así anunciaba el 16 de febrero **Bullrich** la detención de dos personas (dando por sentado que eran culpables, aún sin haber sido juzgadas):

Patricia Bullrich
@PatoBullrich

Detuvimos a los responsables del hackeo de mi cuenta de Twitter. Están a disposición de la Justicia. En Argentina no hay delito sin sanción.

2.310 15:03 - 16 feb. 2017

1.810 personas están hablando de esto

Y así los mostraba la **Policía Federal Argentina**:

Policía Federal Argentina
@PFAOficial

PFA DETUVO A DOS HOMBRES ACUSADOS DE HACKEAR LA CUENTA DE LA MINISTRA DE SEGURIDAD DE LA NACIÓN Y DE LA POLICÍA DE SEGURIDAD AEROPORTUARIA.

39 21:28 - 16 feb. 2017

23 personas están hablando de esto

Nada se hacía referencia, desde las cuentas oficiales, a lo ocurrido con los emails del **Ministerio de Seguridad**. Todo se reducía, según ellos, al Twitter personal de la ministra. Seguían mintiendo, ocultando lo realmente ocurrido.

El procesamiento

El 7 de marzo, el **Centro de Información Judicial** publicó el auto de procesamiento de uno de los dos imputados dictado por el juez federal **Sebastián Ramos**. Con sorpresa encuentro que allí aparece mi nombre:

> 4) Informe n°329/17 de la División Delitos Tecnológicos de la Policía Federal Argentina en el que se hizo saber que el cabo primero en especialidad computación, Jorge Manuel Landajo, realizó tareas de "*ciber-patrullaje*" sobre los perfiles públicos de usuarios de la red social "*Twitter*", respecto al hackeo sufrido por la Sra. Ministra de Seguridad, en la cuenta @PatoBullrich, con el fin de efectuar una correcta protección de los datos y de aquella información que pudiera ser sensible en su contenido.
>
> Ante ello, se obtuvieron capturas de pantalla de las publicaciones efectuadas por el usuario Javier Smaldonde –cuenta @mis2centavos-, quien realizó distintos posteos el 26 de enero de 2017 a partir de las 14:18 horas.

¿»*Ciberpatrullaje*«? ¿Qué significará esa palabra? Recordemos que esto es un auto de procesamiento, no una charla informal entre amigos. ¿Y por qué el «*cabo primero en especialidad computación*» **Landajo** habla de las 14:18 horas, si mi primer tweet sobre el tema (que reproduzco a continuación) fue a las 15:45 horas?

> **#NOalVotoElectrónico #BoletaÚnicaPapelYA** 📮
> @mis2centavos2
>
> El que le hackeó la cuenta a @PatoBullrich, que por favor me desbloquee!!!
>
> 117 3:45 PM - Jan 26, 2017
>
> 37 people are talking about this

El párrafo siguiente del escrito es bastante esclarecedor:

> Dado que dicho usuario mencionaba en reiteradas publicaciones al perfil "*Libero*" –cuenta @LiberoamericaMu- se ingresó a su cuenta de la red social "*Twitter*" y se encontró una publicación realizada el 26 de enero de 2017 a las 15:59 horas con el siguiente contenido "*Momentos antes de resetear la password a la ministra :p*", adjuntándose a dicha publicación una captura de pantalla de la bandeja de entrada de la cuenta de correo patricia.bullrich@minseg.gob.ar y se observa, en pantalla dividida, el contenido de un mensaje de correo electrónico recibido en dicha casilla, donde se visualiza como asunto "*Solicitud de restablecimiento de contraseña*", cuyo remitente es "*Twitter*"

¿Qué llevó al cabo primero **Landajo** a dirigirse a mi cuenta y a incluir capturas de pantalla de mis tweets en su informe? ¿Por qué empezó su búsqueda a partir de mí, para luego llegar al usuario «*Libero*«? Mi asombro aumentó al leer lo siguiente:

> 41) Constancias de migraciones y sistema IDGE de Javier Lorenzo Carlos Smaldone y Sebatián Norberto Vulcano (cfr. fs. 273/89).

¿Por qué se investigaron mis salidas y entradas al país? ¿Por qué investigaron mis antecedentes y vínculos familiares en el **sistema IDGE**? ¿Todo esto por citar o retuitear tweets de otra persona (a quien no parecen haberse esforzado para identificar)? Pero mi sorpresa fue aún mayor cuando encontré en el escrito el nombre de **Alfredo Ortega**:

> 38) Declaración testimonial de Jorge Manuel Landajo, quien manifestó que el día 26 de enero de 2017 a las 18:26 horas observó una publicación del usuario Alfredo Ortega, que se refiere a un "*retwit*" de otro perfil y otro posteo referente al usuario "*Lucas Mercado*", cuyo contenido fue anexado mediante capturas de pantalla (cfr. fs. 251/4).

Alfredo Ortega (doctor en informática del **ITBA** y especialista en seguridad informática reconocido internacionalmente) aparece mencionado… ¡por retuitear un tweet de otra persona! Sí, por dar un RT (una tarde donde **Patricia Bullrich** fue «*trending topic*«). Nuevamente: ¿por qué el cabo primero **Landajo** estaba viendo su perfil, y por qué decidieron incluirlo con nombre y apellido en la causa? Quizás, «*ciberpatrullando*» mis tweets de aquel día, se encontró con este:

#NOalVotoElectrónico #BoletaÚnicaPapelYA 📠
@mis2centavos2

Sobre los sistemas del @MinSeg y la cuenta de @PatoBullrich, recuerden lo que dijo @ortegaalfredo en Diputados:

59 17:38 - 26 ene. 2017

58 personas están hablando de esto

Y la última pregunta: ¿por qué se publican nuestros nombres completos, cuando según las «reglas de Heredia» sólo deberían incluirse nuestras iniciales, ya que no estamos implicados directamente en la causa?

¿»Ciberpatrullaje» dirigido?

Tanto **Alfredo Ortega** como yo fuimos invitados a exponer el año pasado tanto en la **Cámara de Diputados** como en la **Cámara de Senadores**, y en ambas expusimos nuestra posición contraria al **voto electrónico**. Quizás sea esto lo que dirigió al «*cabo primero en especialidad computación*» en su extraño «*ciberpatrullaje*» directamente hacia nuestras cuentas de Twitter. Definitivamente, decir ciertas cosas molesta a muchos.

#NOalVotoElectrónico #BoletaÚnicaPapelYA
@mis2centavos2

Creo que con @ortegaalfredo fuimos tan claros como es posible. Aunque no sirva de nada. #NoAlVotoElectrónico

144 21:44 - 21 nov. 2016

144 personas están hablando de esto

Es inquietante pensar hasta dónde llegará el «*ciberpatrullaje*» que realizan las fuerzas de seguridad comandadas por la ministra **Patricia Bullrich** y cuántas veces pasarán las «*ciberpatrullas*» por nuestros perfiles en redes sociales sin que nos enteremos. Claro, no están identificadas por ningún color, y no llevan balizas ni sirenas.

Javier Smaldone
@mis2centavos

¿Por qué aparece la filtración de 700 Gb de datos de #LaGorraLeaks? Porque durante 2 años, @PatoBullrich y la @PFAOficial no hicieron NADA. Abro hilo. 👇

189 20:29 - 12 ago. 2019

146 personas están hablando de esto

Javier Smaldone
@mis2centavos

En respuesta a @mis2centavos

En enero de 2017 alguien identificado como [S] hackeó la cuenta de twitter de @PatoBullrich. Pero no sólo eso, sino también su cuenta de email y otras del @MinSeg y de la @PFAOficial.

22 20:29 - 12 ago. 2019

Ver los otros Tweets de Javier Smaldone

Javier Smaldone
@mis2centavos

En respuesta a @mis2centavos

La ministra cosplayer lanzó una serie de allanamientos y detenciones contra algunos perejiles, y también mandó al cabo Landajo a "ciberpatrullar" a algunos que les resultábamos antipáticos.
(La historia la conté acá: blog.smaldone.com.ar/2017/03/09/pat…)

Patricia Bullrich y el «ciberpatrullaje»
El 26 de enero de 2017 a la ministra de Seguridad Patricia Bullrich le "hackearon" su cuenta de Twitter. Horas después, apareció
blog.smaldone.com.ar

28 20:29 - 12 ago. 2019

Ver los otros Tweets de Javier Smaldone

Javier Smaldone
@mis2centavos

En respuesta a @mis2centavos y 2 más

Si algún periodista quiere investigar (y ver lo que declaré en la testimonial): Expediente 1033 / 2017, "MIRCO MILSKI, RICARDO DAMIAN Y OTROS s/INTIMIDACION PUBLICA. DAMNIFICADO: BULLRICH, PATRICIA Y OTROS", Juzgado Criminal y Correccional Federal 2, Comodoro Py 2002, 3° piso.

31 20:36 - 12 ago. 2019

Ver los otros Tweets de Javier Smaldone

Javier Smaldone
@mis2centavos

En respuesta a @mis2centavos

Sí, ya sé que está la contraseña. Pero deberían haberla cambiado, porque hace más de 2 años llevé todo esto al juez en Comodoro Py y di una declaración testimonial. En la misma, dejé constancia de que estaban persiguiendo perejiles y haciendo teatro para los medios.

24 20:30 - 12 ago. 2019

Ver los otros Tweets de Javier Smaldone

Javier Smaldone
@mis2centavos

En respuesta a @mis2centavos

[S] seguía libre, mientras se estaba exponiendo, escrachando, allanando y deteniendo a inocentes. Hasta ese momento, [S] no había querido hacer daño: podría haber vendido, usado o publicado esa información, pero en cambio quiso hacerla llegar a periodistas para INFORMAR.

21 20:30 - 12 ago. 2019

Ver los otros Tweets de Javier Smaldone

Javier Smaldone
@mis2centavos

En respuesta a @mis2centavos

Luego [S] desapareció. Pero aparentemente los sistemas de la @PFAOficial siguieron siendo tan vulnerables como siempre, y ahora hace este desastre: publicar 700 Gb de datos que pueden poner en riesgo las vidas de mucha gente inocente. Seguí tribuneando, @PatoBullrich.

37 20:30 - 12 ago. 2019

17 personas están hablando de esto

Javier Smaldone
@mis2centavos

En respuesta a @mis2centavos y 2 más

Si algún periodista quiere investigar (y ver lo que declaré en la testimonial): Expediente 1033 / 2017, "MIRCO MILSKI, RICARDO DAMIAN Y OTROS s/INTIMIDACION PUBLICA. DAMNIFICADO: BULLRICH, PATRICIA Y OTROS", Juzgado Criminal y Correccional Federal 2, Comodoro Py 2002, 3° piso.

31 20:36 - 12 ago. 2019

Ver los otros Tweets de Javier Smaldone

#GraciasPatoBullrich

Sr. Juez Federal:

Javier Lorenzo Carlos Smaldone, conjuntamente con mi abogado defensor, Pablo Slonimsqui, en la causa que lleva el n° 55276/2019 del registro de la Secretaría n° 18 de este Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en el Pasaje Rodolfo Rivarola 193, piso 3° oficina 11 de esta Ciudad Autónoma de Buenos Aires, ante V.S. me presento y digo:

Que vengo por intermedio de este escrito a acompañar a este legajo, ampliando las presentaciones hechas días pasados, para explicarle a V.S. la única mención a mi persona que aparece en el expediente de autos que no parece provenir de las sospechas infundadas de la fuerza policial.

En el informe de "ciberpatrullaje" de la Policía Federal Argentina del día 20 de agosto de 2019 —a fs. 224— se incluye una captura de pantalla del canal de Telegram atribuido al autor de la filtración donde aparece un mensaje del mismo diciendo *"Siempre @mis2centavos dando cátedra"* (en alusión a mi nombre de usuario en la red social Twitter) seguido de un tweet mío donde propongo mejoras al sistema de escrutinio electoral.

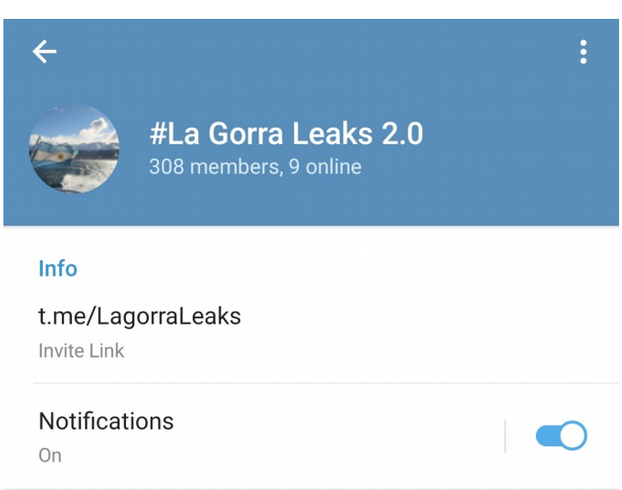
Esta, insisto, es la única mención a mi persona en todo el expediente que a simple vista no parece provenir de las retorcidas elucubraciones o las mentiras flagrantes de la Policía, sino de quien realizó la filtración de archivos sensibles (identificado como *"La Gorra Leaks 2.0"*). Lo que los investigadores policiales omiten decir —y que claramente se desprende de la información vertida en sus propios informes— es que dicho canal de Telegram el día 20 de agosto no se encontraba bajo el control de esta persona, sino de Rodrigo Gimenez. A continuación, la prueba:

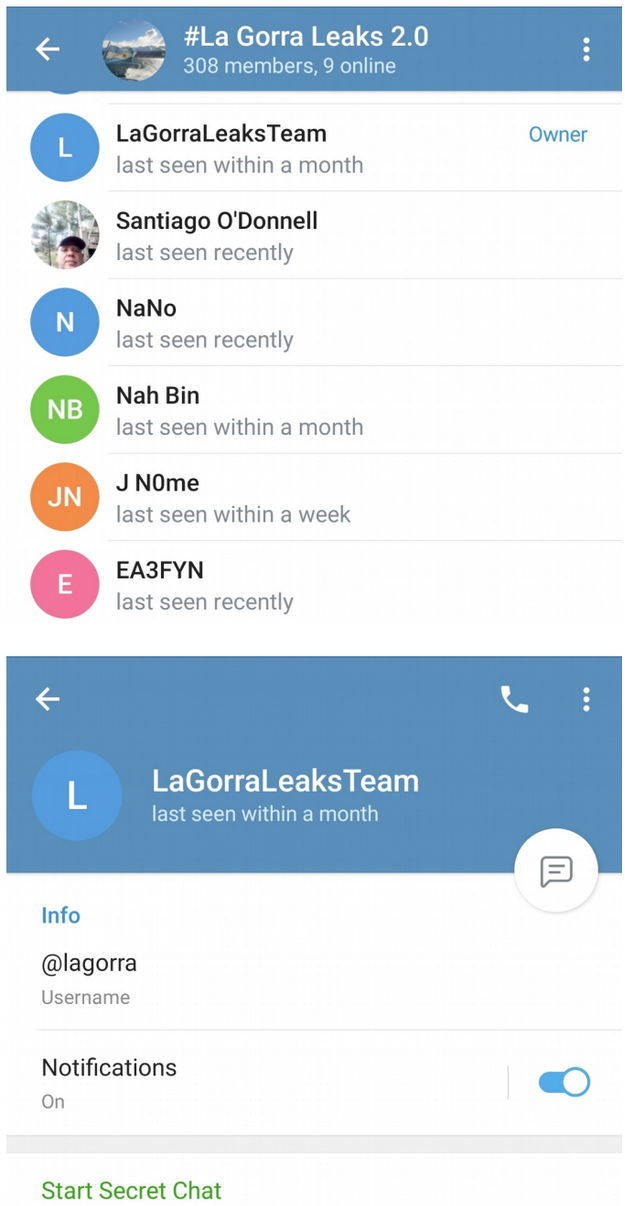
1) En el último párrafo de fs. 236 el informe policial dice que el canal de Telegram para difundir la filtración fue creado el día 11 de agosto de 2019.

2) En la última captura de pantalla del repositorio de archivos de la "dark web" (no "deep web") Tor de fs. 223, de fecha 19 de agosto de 2019, aparece el contenido del archivo "TELEGRAM.TXT" donde se lee lo siguiente: *"Mis canales en Telegram fueron borrados. Los nuevos canales no son administrados por mi, no son mios. Todo lo que se publica alli es fake. [S]"*. Si bien no se puede asegurar la veracidad de tal afirmación, sí puede tenerse la certeza de que provino de alguien con la capacidad de publicar material en ese repositorio.

3) La captura de fs. 360 de la cuenta de Telegram tiene el nombre de usuario "**@gorraleaks**". La misma fue utilizada el 11 de agosto para crear el canal de Telegram "**LagorraLeaks**", mediante la cual se realizó la difusión de la filtración (enlaces al repositorio en la "dark web" Tor) atribuida.

4) Una verificación que aún hoy puede hacerse —ya que todavía existe— muestra que el canal de Telegram **"LagorraLeaks"** es administrado por la cuenta "**@lagorra**".





5) El informe policial que comienza en fs. 445 diferencia los canales de Telegram según su nombre de descriptivo: *"La Gorra Leak 2.0"* y *"LaGorraLeak2.0"*. Esto es engañoso, ya que lo que identifica unívocamente a un canal de Telegram es su nombre (**"LagorraLeaks"**, como puede verse en la primera captura de pantalla del punto anterior) y no su descripción (que incluso puede variar en el tiempo).

6) El señor Rodrigo Gimenez reconoce, según lo dicho en fs. 440. y en la nota de INFOBAE citada, ser el autor de la segunda cuenta de Telegram ("**@lagorra**") y del nuevo canal ("**LagorraLeaks**") que cuyo nombre coincide con el originalmente utilizado para realizar la filtración —ya inexistente para ese momento— pero cuya descripción es diferente (contiene espacios).

En resumen, el autor de la filtración utilizó un canal de Telegram llamado "**LagorraLeaks**", creado el 11 de agosto de 2019 y administrado desde una cuenta de Telegram llamada "**@gorraleaks**". Por algún motivo, dicho canal desapareció alrededor del 17 de agosto de 2019. Allí aparece el señor Gimenez, creando otro canal con el mismo nombre ("**LagorraLeaks**"), pero utilizando un usuario diferente ("**@lagorra**") e inicialmente simulando ser la misma persona que difundía la filtración en el canal anterior. Es entonces cuando envía un mensaje alabándome y citando uno de mis tweets. Desconozco cual fue su motivación para hacerlo, pero sí es claro que los investigadores policiales se valieron de esto para intentar sumar un elemento en mi contra relacionándome con el autor de la filtración.

Este "cambio de canales" ocurrido el 17 de agosto fue notado por varios en la red social Twitter (incluso algunos periodistas me alertaron sobre la mención a mi cuenta), por lo que

que creí que se trataba de otra maniobra policial tendiente a involucrarme (como puede verse en mis tweets citados en fs. 225 y 231). Ahora, viendo el expediente, puedo confirmar mi sospecha: los investigadores eran conscientes que se se trataba de dos canales distintos, administrados por personas distintas, pero no lo hicieron notar. Seguramente por eso omitieron incluir en el informe de "ciberpatrullaje" este tweet que emití por esos días:

https://twitter.com/mis2centavos/status/1163857336173301761

En virtud de los expuesto, habré de solicitar a V.S. tenga en cuenta cuanto se dice en este escrito, en consonancia con lo manifestado en anteriores presentaciones, y al resolver lo haga de modo solicitado por esta parte.

Proveer de conformidad,
SERÁ JUSTICIA.

#GraciasPatoBullrich

Sr. Juez Federal:

Pablo Slonimsqui, abogado defensor del señor Javier Lorenzo Carlos Smaldone, en la causa que lleva el nº 55276/2019 del registro de la Secretaría nº 18 de este Juzgado Nacional en lo Criminal y Correccional Federal nº 9, manteniendo el domicilio constituido en el Pasaje Rodolfo Rivarola 193, piso 3º oficina 11 de esta Ciudad Autónoma de Buenos Aires, ante V.S. me presento y digo:

Que vengo por intermedio de este escrito a acompañar al legajo, el comunicado dado a conocer días pasados por distintas organizaciones de la sociedad civil, académicas y particulares dedicados al estudio de políticas públicas de Internet y a la defensa de derechos fundamentales, mediante el cual se expresar su preocupación frente a los reiterados casos de persecución a investigadores de seguridad digital.

En esta oportunidad, puede verse, el caso que ha llamado la atención de dichas organizaciones a nivel local e internacional es la investigación a respecto de mi defendido, investigador en seguridad informática, divulgador y reconocido vocero de la campaña pública #NoAlVotoElectrónico.

En el caso de Javier Smaldone, se afirma en dicho comunicado, su opinión técnica y crítica no debería ser vista como sospechosa, sino como una demostración de sus conocimientos técnicos y su pasión por la seguridad de los sistemas informáticos.

La libertad de expresión abarca el derecho a impartir información, es decir, a publicar y alertar sobre la existencia de vulnerabilidades en sistemas informáticos, con el objetivo de concientizar para su solución. Existe también aquí un interés social en conocer sobre fallas en sistemas esenciales para el ejercicio y la protección de los derechos de los ciudadanos.

Las ORGANIZACIONES FIRMANTES pertenecen más de diez países y son: **Access Now** (Internacional, https://www.accessnow.org/) **Asociación de Software Libre** (Ecuador, https://www.asle.ec/) **Centro de Estudios Legales y Sociales** (Argentina, https://www.cels.org.ar/web/) **Cooperativa Tierra Común** (México, https://tierracomun.org/) **Datos Protegidos** (Chile, http://www.datosprotegidos.org/) **Derechos Digitales** (Latinoamérica, https://www.derechosdigitales.org/) **Electronic Frontier Foundation** (Estados Unidos, https://www.eff.org/) **Fundación Acceso** (Centroamérica, http://www.acceso.or.cr/) **Fundación Internet Bolivia** (Bolivia, https://internetbolivia.org/) **Fundación Karisma** (Colombia, https://karisma.org.co/) **Fundación Via Libre** (Argentina, https://www.vialibre.org.ar/) **Hiperderecho** (Perú, https://hiperderecho.org/) **Intervozes** (Brasil, https://intervozes.org.br/) **Nodo TAU** (Argentina, https://tau.org.ar/) **Poder Ciudadano** (Argentina, http://poderciudadano.org/) **Red en Defensa de los Derechos Digitales R3D** (México, https://r3d.mx/) **Sursiendo** (México, https://sursiendo.com/) TEDIC (Paraguay, https://www.tedic.org/) y **Usuarios Digitales** (Ecuador, http://www.usuariosdigitales.org/).

En la inteligencia que se trata de voces particularmente autorizadas en un tema específico de máximo interés a nivel global, y en tanto dicho comunicado culmina rechazando toda persecución a investigadores informáticos y solicitando expresamente a la justicia que revise lo actuado por las fuerzas de seguridad **en este caso, y restituya a mi defendido sus elementos de trabajo sin avanzar en la vulneración de sus derechos fundamentales,** parece oportuno a esta defensa acompañar dicho texto al legajo.

Tener presente lo expuesto,

SERA JUSTICIA

Ciudad Autónoma de Buenos Aires, 1 de noviembre de 2019

Atte.
Juez Federal, Luis Rodriguez
Ministra de Seguridad, Patricia Bullrich

Quienes suscriben, organizaciones de la sociedad civil, académicas y particulares dedicados al estudio de políticas públicas de Internet y a la defensa de derechos fundamentales, nos dirigimos a ustedes para expresar nuestra preocupación frente a los reiterados casos de persecución a investigadores de seguridad digital. En esta oportunidad, el caso que ha llamado la atención de nuestras organizaciones a nivel local e internacional es la investigación a Javier Smaldone, investigador en seguridad informática, divulgador y reconocido vocero de la campaña pública #NoAlVotoElectrónico.

Recientemente, la Justicia Federal de la República Argentina ordenó el allanamiento de su domicilio a pedido de la Policía Federal Argentina, fuerza que depende de la Ministra de Seguridad, Patricia Bullrich.

La causa judicial en la que se amparó el allanamiento es la investigación por la filtración de datos de las fuerzas de seguridad en agosto de este año, relacionada por la policía con la filtración ocurrida en 2017. Según se supo públicamente, en este último caso los datos habrían sido obtenidos haciendo uso de la técnica conocida como “phishing”. Este método habría consistido en la creación de una cuenta falsa a nombre de la Superintendencia de Bienestar de la Policía Federal Argentina por la que los perpetradores habrían logrado acceder a los datos de usuario y contraseña de la víctima. Posteriormente se habría utilizado esta información para acceder a la base datos donde se conservaba información sensible de las fuerzas de seguridad para luego publicarla en redes sociales. Este caso recibió el nombre de “La Gorra Leaks 2”.

Según el expediente de la causa, al no obtener las fuerzas de seguridad datos concretos sobre quien o quienes habían accedido ilícitamente a sus bases de datos, comenzaron a observar “fuentes abiertas y redes sociales” para detectar usuarios que hubieran replicado la difusión de esta información.

En este contexto, surge del expediente que Javier Smaldone es señalado como uno de los “posibles responsables” de los hechos a pesar de no haber sido imputado, y haber declarado previamente como testigo aportando información valiosa a la Justicia. Los indicios presentados por la policía en este sentido llaman la atención de la comunidad y del público por su arbitrariedad y debilidad. En primer lugar, convierten en presunto sospechoso a Smaldone por el mero hecho de tener conocimientos especializados en seguridad informática y, en segundo lugar, sospechan de su participación en este acto por las publicaciones que realizó en redes sociales y sus opiniones respecto del caso (véase “indicios” página 5 del expediente). El juez de la causa consideró suficientes estos indicios para autorizar el acceso a información sensible de Smaldone, incluyendo el requerimiento de su geolocalización a proveedores de telefonía móvil, la intervención de sus comunicaciones privadas, la instalación de cámaras de vigilancia en los alrededores de su domicilio, la solicitud de seguimiento de sus movimientos a partir de informes sobre el uso de su tarjeta de transporte público, el allanamiento de su domicilio, el secuestro de sus dispositivos personales y herramientas de trabajo y su demora por 6 horas para la presunta investigación de antecedentes de los que carece.

De los indicios señalados, sin embargo, no se desprende ningún hecho o circunstancia sólidas que revistan carácter suficiente para constituir una sospecha fundada que autorice las graves medidas emprendidas. La Corte Suprema de Justicia Argentina ya afirmó que la intervención y el acceso a datos relativos a la comunicación deben cumplir con un análisis suficiente de necesidad y proporcionalidad de la restricción del derecho del investigado. Asimismo el Código Procesal Penal Federal establece la razonabilidad como parte del examen que debe hacer el juez cuando autorice medidas de comprobación directas como el allanamiento (art. 144).

Tanto el estándar legal para acceder a los datos, como la necesidad y proporcionalidad de las medidas, son requisitos establecidos en estándares internacionales de derechos humanos. Así lo explican los “Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones”[1], producto de una consulta global con grupos de la sociedad civil, la industria y expertos en la materia. Esos principios establecen que toda medida que implique una privación de un derecho fundamental sólo puede estar justificada cuando es prescrita por la ley, es **necesaria** para lograr un objetivo legítimo, y es **proporcional** al objetivo perseguido.

Lamentablemente, este no es el primer caso de investigación penal sin fundamentos suficientes contra investigadores de seguridad informática en Argentina. En 2016 Joaquín Sorianello[2] fue sobreseído por la justicia luego de haber sido allanado y procesado por haber alertado sobre las vulnerabilidades en el software de la Boleta Única Electrónica. De forma similar, Iván Barrera Oro[3] fue allanado en 2016 acusado de “producción y tráfico de pornografía infantil” coincidentemente luego de haber demostrado la posibilidad de cargar hasta 20 votos por boleta entre otras deficiencias. En 2017 fue sobreseído.

Este accionar de la justicia se encuentra en oposición a su obligación de garantizar el debido proceso, proteger los derechos individuales garantizados por la Constitución Nacional (entre ellos la libertad de expresión y la privacidad) y tratados internacionales, y a fundamentar debidamente sus decisiones cuando las medidas a adoptar impliquen una limitación a esos derechos.

El trabajo de los investigadores en seguridad informática está protegido por el derecho a la libertad de expresión. Esto surge de la interpretación amplia de la jurisprudencia y la doctrina del artículo 13 de la Convención Americana de Derechos Humanos. Es un comportamiento usual para los investigadores monitorear, comentar y criticar información relacionadas a su expertise técnico en las redes sociales o en medios periodísticos. Por eso, en el caso de Javier Smaldone, su opinión técnica y crítica no debería ser vista como sospechosa, sino como una demostración de sus conocimientos técnicos y su pasión por la seguridad de los sistemas informáticos. Más aún, y específicamente en relación al caso de Smaldone, la libertad de expresión abarca el derecho a impartir información, es decir, a publicar y alertar sobre la existencia de vulnerabilidades en sistemas informáticos, con el objetivo de concientizar para su solución. Existe también aquí un interés social en conocer sobre fallas en sistemas esenciales para el ejercicio y la protección de los derechos de los ciudadanos.

Contrariamente a lo que sucedió en este caso, la justicia debería tener la responsabilidad de controlar lo actuado por las fuerzas de seguridad en todo proceso de investigación criminal y garantizar la protección de los derechos fundamentales. Ello implica desechar solicitudes temerarias, rechazar los avances sobre la vida privada de las personas sin sospechas debidamente fundadas y evitar la utilización del sistema penal como respuesta al trabajo de los investigadores en seguridad informática.

Por lo antedicho, rechazamos toda persecución a investigadores informáticos y respetuosamente instamos a que se respete el ejercicio a la libertad de expresión que su actividad implica. En ese sentido, solicitamos a la justicia que revise lo actuado por las fuerzas de seguridad en el caso de Javier Smaldone y restituya sus elementos de trabajo sin avanzar en la vulneración de sus derechos fundamentales.

1 https://necessaryandproportionate.org/es/necesarios-proporcionados
2 https://www.lanacion.com.ar/tecnologia/sobreseyeron-al-programador-que-revelo-fallas-en-el-sistema-de-boleta-unica-electronica-nid1924088
3 https://www.derechosdigitales.org/wp-content/uploads/1.Legal-Informe-Argentina.pdf

ORGANIZACIONES FIRMANTES

Access Now (Internacional, *https://www.accessnow.org/*)
Asociación de Software Libre (Ecuador, *https://www.asle.ec/*)
Centro de Estudios Legales y Sociales (Argentina, *https://www.cels.org.ar/web/*)
Cooperativa Tierra Común (México, *https://tierracomun.org/*)
Datos Protegidos (Chile, *http://www.datosprotegidos.org/*)
Derechos Digitales (Latinoamérica, *https://www.derechosdigitales.org/*)
Electronic Frontier Foundation (Estados Unidos, *https://www.eff.org/*)
Fundación Acceso (Centroamérica, *http://www.acceso.or.cr/*)
Fundación Internet Bolivia (Bolivia, *https://internetbolivia.org/*)
Fundación Karisma (Colombia, *https://karisma.org.co/*)
Fundación Via Libre (Argentina, *https://www.vialibre.org.ar/*)
Hiperderecho (Perú, *https://hiperderecho.org/*)
Intervozes (Brasil, *https://intervozes.org.br/*)
Nodo TAU (Argentina, *https://tau.org.ar/*)
Poder Ciudadano (Argentina, *http://poderciudadano.org/*)
Red en Defensa de los Derechos Digitales R3D (México, *https://r3d.mx/*)
Sursiendo (México, *https://sursiendo.com/*)
TEDIC (Paraguay, *https://www.tedic.org/*)
Usuarios Digitales (Ecuador, *http://www.usuariosdigitales.org/*)

#GraciasPatoBullrich

Sr. Juez Federal:

Javier Lorenzo Carlos Smaldone, conjuntamente con mi abogado defensor, Pablo Slonimsqui (23-21142410-9), en la causa que lleva el n° 55276/2019 del registro de la Secretaría n° 18 de este Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en el Pasaje Rodolfo Rivarola 193, piso 3° oficina 11 de esta Ciudad Autónoma de Buenos Aires, Ante V.S. me presento y digo:

Que he podido acceder al dictamen del Ministerio Público Fiscal mediante el cual se propició el rechazo del planteo de nulidad oportunamente interpuesto por esta parte.

En este escenario, no pudiendo dejar de destacar mi asombro —aún sin ser abogado, Monesvol no lo permita— cuando leo que en opinión del Fiscal *la valoración de los indicios para determinar si hay motivo para vulnerar la inviolabilidad del domicilio es "de otra etapa procesal"*.

Entonces me pregunto: ¿Cuándo vamos a discutirlo? ¿Cuando los efectos que se intentan evitar se encuentren ya consumados?

Así, dice el fiscal que la entidad de los informes policiales y de las demás constancias se ven jaqueadas por apreciaciones que, a esta altura parecen más de una discusión sobre el mérito de la prueba, más que el valor primario y reciente que tienen las definiciones del actuar prevencional para fundamentar la diligencia cautelar.

No tengo ninguna intención de polemizar en esta instancia con el Fiscal, pero no puedo menos que dejar constancia del estupor que produce que, quien está llamado por la Constitución Nacional a velar por la legalidad de todos los procesos judiciales en los que interviene, entienda que la demostración palmaria acerca de informes policiales notoriamente falsos, basados sobre hechos inexistentes y mentiras, orientados por razones inconfesables que se vinculan con un evidente encono de algún sector de las fuerzas policiales para conmigo, sea considerada como una discusión sobre el mérito de la prueba.

Cuando el fiscal afirma que "Los elementos tenidos en cuenta para el allanamiento fueron el resultado del estudio previo de las constancias recolectadas" deja en claro que o no entendió el planteo de esta parte, o evidentemente no leyó el legajo.

Parece inverosímil la premisa que defiende el Ministerio Público, por cuanto postula un principio inaceptable —por lo menos en un lugar civilizado: *Allano ahora, ya luego tendré ocasión de analizar si había motivos para allanar.*

Ya he señalado de forma incontestable todas las razones que permiten rechazar los argumentos —por llamarlos de alguna manera— exteriorizados por el personal policial que colabora —también por decirlo de alguna manera— con la presente investigación a los fines de involucrarme en la misma.

Solo diré aquí que, buscando entre los restos del naufragio, en vez de preocuparse por la inaceptable violación de derechos que trasluce la actuación policial, el Ministerio Público intenta rescatar un indicio, en concreto un supuesto tweet (cuya existencia no puede chequearse ni en Twitter ni en el expediente) que "prima facie" constituiría una situación que puede sustentar la diligencia.

Probablemente el Sr. Fiscal no entiende la dinámica de las redes sociales, ni nadie de su equipo lo ha asesorado al respecto: es la única explicación que puedo encontrar para que

alguien, de buena fe, considere que un intercambio de tweets, sobre una cuestión que en nada se vincula con los hechos que interesan a esta investigación, pueda justificar una orden de allanamiento.

Se trata, vale la pena recordarlo, de un supuesto tweet —que no aparece por ningún lado— mediante el cual yo le habría contestado —antes de que se verifiquen los hechos que aquí se investigan— a una persona (Capitan_Alfa), alguna cosa vinculada con temas de seguridad de satélites.

Dicho esto, señalo que por día intervengo en innumerables conversaciones de las características de la que aquí nos ocupa, desde hace más de diez años, y seguramente el Capitan_Alfa debe haber recibido un montón de respuestas de gente que no ha sido allanada, por razones que no hace falta, entre adultos, explicar.

Seriamente hablando, a nadie sensato se le puede ocurrir invocar como fundamento válido para un allanamiento un intercambio de tweets de la naturaleza del que nos ocupa.

He leído varias veces el dictamen en comento, y lo encontré extraordinariamente malo. De dimensiones modestísimas, se fuerza hasta el absurdo una línea argumental con el objeto inocultable de encontrar una respuesta, aunque no sea la correcta, que justifique el aberrante accionar policial que exhibe el legajo.

Lamentablemente, en esta ocasión, el Ministerio Público ha puesto en evidencia, también, una inclinación tendiente a adoptar formatos de intervención que eviten involucrarse en discusiones intelectualmente exigentes.

En fin, más de lo mismo. Otra vez sopa.

Dígnese V.S. tener presente lo expuesto, SERÁ JUSTICIA.

INTERPONE RECURSO DE APELACIÓN. RESERVAS.

Sr. Juez Federal:

Pablo Slonimsqui, abogado defensor del Sr. Javier Lorenzo Carlos Smaldone, en la causa que lleva el nº 55276/2019 del registro de la Secretaría nº 18 de este Juzgado Nacional en lo Criminal y Correccional Federal nº 9 —**Incidente nº 3**—, manteniendo el domicilio constituido en el Pasaje Rodolfo Rivarola 193, piso 3º oficina 11 de esta Ciudad Autónoma de Buenos Aires, ante V.S. me presento y digo:

I

Que vengo por intermedio del presente, en legal tiempo y forma, y conforme expresamente lo autoriza la normativa procesal vigente, a interponer el correspondiente recurso de apelación en contra de lo resuelto por el Tribunal con fecha 18 de diciembre pasado, en tanto dispuso rechazar el planteo de nulidad interpuesto por esta parte.

Dicha resolución, por sus características, causa a esta parte un gravamen irreparable.

Ello así, conforme los argumentos de hecho y de derecho que seguidamente expondré.

II

Se iniciaron las presentes actuaciones con fecha 30 de julio pasado, cuando la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina puso en conocimiento de la justicia los episodios que conforman el objeto procesal de estos actuados.

Así, conforme se desprende del testimonio de Claudio Ricardo Ramos, Subcomisario con funciones en la dependencia señalada, quien refirió que el 29 de julio pasado se recibió en varias dependencias de la Policía Federal un correo electrónico que simulaba provenir de la Superintendencia de Bienestar, el cual contenía un enlace que al ser accionado re-direccionaría a un formulario el cual solicitaba se completen datos personales y demás información.

Se trata de una maniobra conocida como “*phishing”* y permite sustraer datos.

Luego, a través del Ministerio de Seguridad de la Nación, se tomó conocimiento que en la red social Twitter un usuario @lagorraleaks refirió haber subido a la Deep Web información relacionada con la Policía Federal, específicamente de las áreas de bienestar y drogas peligrosas, razón por la cual se supone que la información allí publicada puede ser la obtenida a través del mecanismo antes descripto.

La Deep Web, se aclara, es un área de internet sin control por parte de las empresas internacionalmente conocidas como Google y donde resulta muy difícil rastrear a los usuarios e información que allí se vuelca.

A partir de las alertas emitidas por la empresa Gmail se pudieron individualizar dos IPs que se corresponderían con las conexiones utilizadas por la persona que habría obtenido los datos de forma engañosa tras ingresar en la cuenta oficial de la Policía Federal sin autorización.

Y, siempre en el concepto del Subcomisario Ramos, teniendo en cuenta la modalidad y tipografía utilizadas por el usuario de Twitter @lagorraleaks2.0, se lo puede relacionar con las personas que en el año 2017 hackearon la cuenta de la Ministra Patricia Bullrich.

Sobre esta base, se dio curso a una investigación tendiente a individualizar a los autores del hecho —cuya gravedad no solo nadie discute, sino que incluso mi defendido puso de manifiesto públicamente a través de su cuenta de Twitter inmediatamente de conocidos los acontecimientos—, investigación que muestra como dato significativo, de un modo evidente, manifiesto, notorio y ostensible, la intención de vincular al Sr. Smaldone con estos episodios, aun cuando para ello haya que recurrir a métodos que resultan particularmente infantiles.

III

Puede verse de lo actuado que, a la par de una investigación en apariencia racional y estructurada sobre elementos objetivos de análisis, mediando una creatividad de dimensiones modestísimas se pretendió ubicar a mi defendido como responsable de algo —de cualquier cosa— vinculado con

los hechos investigados, aun cuando surge nítido del legajo su total ajenidad respecto de los mismos.

Y digo así, puesto que habiendo compulsado las actuaciones —por momentos con profundo asombro—, no solo no se advierte que elemento probatorio podría eventualmente sustentar una imputación en contra del Sr. Smaldone, sino que tampoco se advierte en concreto —ni en abstracto— cuál sería el hecho que se le imputa.

A fs. 67/68 puede verse un informe remitido al Tribunal por la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina, donde se refieren las medidas de investigación realizadas sobre las máquinas de las dependencias policiales vulneradas, y se da cuenta de los progresos de la investigación estructurados a partir de dicho análisis.

Nada que decir sobre ello.

Pero el problema empieza cuando en dicho informe se anuncia que *teniendo en cuenta la posibilidad de que el autor de la maniobra pueda involucrar mayor cantidad de información y hacerla pública, es que personal nuestro se halla avocado* (sic) *a la observación de fuentes abiertas y redes sociales, detectando ciertos usuarios que habrían replicado la publicación en distintas redes sociales y sistemas de chat con la vulnerabilidad investigada.*

Y sigue el informe:

En otro orden de cosas se destaca que esta División llevó a cabo las investigaciones en torno a los hechos suscitados en el año 2017, relacionado al acceso a la cuenta particular de red social Twitter de la Ministra de Seguridad de la Nación generada con el mismo modus operandi investigado en este caso, teniendo en cuenta la existencia actual del usuario de la red social TWITTER denominado @Lagorraleaks2.0, que no solo hace público los datos obtenidos de las dependencias afectadas de esta Policía Federal, sino que también se atribuye los hechos ocurridos en el año 2017 de la siguiente manera: "En enero del 2017 conseguí acceso a varios correos electrónicos del Ministerio de Seguridad, uno de ellos fue el de la actual ministra de seguridad, Patricia Bullrich, a través del cual tomé su cuenta en twitter. Meses más tarde publiqué los emails de varias fuerzas, que se conoció como "lagorraleaks". Defacee la web del ejército (o fue ISIS?), gendarmería, policía de la ciudad y hackee al diputado tonelli"

Ante esta situación, habiéndose comprobado la autoría de los autores involucrados en el hecho del hackeo a la cuenta de Twitter de la Ministra en el año 2017, y la capacidad técnica que estos presentan para llevar a cabo los presentes hechos, y habiendo encontrado publicaciones donde se adjudican estos al mismo tiempo, se considera a estos como posibles responsables del hecho, tratándose de las siguientes personas:

...

...

Javier Smaldone

Este informe es sencillamente escandaloso por una razón elemental: en ningún momento mi defendido ha sido imputado por la justicia por el hackeo a la cuenta Twitter de la Ministra de la Nación, circunstancia que puede verificarse mediante la compulsa de las actuaciones correspondientes, que llevan el nº 1033/17 del registro del Juzgado Nacional en lo Criminal y Correccional Federal nº 2, Secretaria nº 4. Todo lo contrario, en dicho legajo el Sr. Smaldone se presentó espontáneamente, se le recibió declaración testimonial, acompañó toda la información que consideró útil y pertinente para dicha investigación y colaboró con la justicia en todo cuanto estuvo a su alcance.

Oportunamente se adjunto copia de dicha declaración a estos actuados.

Por tal motivo, en la evidencia que se ha incorporado a este expediente un informe que contiene información objetivamente falsa, y que a la postre permitió que progresara una insólita imputación en contra del Sr. Smaldone, esta parte solicitó que sin perjuicio del trámite de las presentes actuaciones, se extraigan testimonios y se formule la denuncia correspondiente a los fines de investigar las razones que motivaron la presentación referida y la identidad de los ideólogos de tan patética estrategia.

Ello, teniendo en especial consideración que a partir de la incorporación de datos mentirosos en un expediente judicial (la policía se permitió el lujo táctico de inventar cosas) se desarrolló una investigación sobre la persona de mi defendido —desproporcionada en si misma, y de una intensidad muy superior a la que se verificó respecto del resto de los imputados— inadmisible

en un estado democrático, cuyas verdaderas motivaciones exceden por mucho, la declamada necesidad de investigar los hechos que integran esta causa.

Como se dijo oportunamente, se han intentado múltiples alternativas para incriminar al Sr. Smaldone, ninguna con éxito.

Y alguien debería responder por semejante atropello.

Retomando el curso de este legajo, podemos ver que a fs. 93/4 obra nuevamente dicho informe de la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina.

Luego, en el marco de un extenso informe se da cuenta que el ciberpatrullaje sobre la cuenta @mis2centavos no presenta datos de interés (fs.221) y que se detectó que un grupo creado dentro de la red social Telegram llamado “La gorra Leaks Team” y “Lagorraleaks 2.0”, comparte tweets de @mis2centavos en temas relacionados a “las elecciones 19”.

Menciones de la cuenta de mi defendido cuya vinculación con estos actuados no se alcanza a comprender pueden verse a fs. 224/vta., 225, 225, 227 y 231. Se trata, en lo esencial, de opiniones políticas y conceptos técnicos que interesan a quienes se dedican a la informática.

Llegamos así al informe obrante a fs. 236/43, mediante el cual la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina repasa los antecedentes de su tarea en el caso, y en cuanto aquí interesa señala que:

Por todo lo expuesto, hasta el momento se puede confirmar a prima face (sic) *dos tipos de acciones delictivas hacia las instituciones y funcionarios públicos.*

Uno de los ataques es la realizada a la seguridad informática de la Policía Federal Argentina (en el caso que nos ocupa), Prefectura Naval Argentina y a la Policía de la Ciudad, la cual dejó vulnerable la Seguridad Nacional ante los ciudadanos.

El segundo ataque se realizó con la utilización de las distintas redes sociales, portales públicos, plataformas de la web, etc; publicaciones que no solo dejan al descubierto documentos y/o datos sensibles y privados, sino

que fomentan en sus comentarios e instigan a un accionar ciudadano contra las instituciones y funcionarios del Estado Nacional y de las Fuerzas Armadas y de Seguridad.

Es por ello, que el presente hecho delictivo derivó en 2 (dos) líneas principales de investigación: una el seguimiento de los resultados de los datos que arrojaron los servidores vulnerados y la otra línea investigativa sobre el monitoreo/análisis de las publicaciones por el atacante informático, como así también sobre otras publicaciones que puedan relacionarse a las mismas (posteos, comentarios, retwitteos, compartimiento de enlaces, etc).

Expresado el hecho, se observó en las publicaciones del atacante una posible relación con el hackeo efectuado a la Sra. Ministra de Seguridad de la Nación, en el año 2017, en virtud que la intromisión al correo de la Sra. Ministra fue realizada en dicho año por quien se autodenominada "La Gorra Leaks", ilícito investigado por la Policía Federal Argentina, específicamente por la División Delitos Tecnológicos del Departamento CIBERCRIMEN, que era comandado por el Comisario Víctor Chanenko, quienes eran los encargados de la investigación en 2017 y a los que se mencionan despectivamente en las publicaciones que nos ocupan.

Atento a ello, como dato de interés se vinculó a la investigación las personas que posiblemente tuvieron alguna relación con el hecho investigado en el año 2017, procediéndose a realizar búsquedas de publicaciones de los mismos en los distintos portales de fuentes abiertas y/o redes sociales, a fin de poseer algún dato de interés a la causa, siendo las personas a considerar:

...

...

Javier Smaldone (el cual utiliza la cuenta @misdoscentavos). El mismo se presentó en su momento en la causa del año 2017 (hackeo a la Ministra de Seguridad) al enterarse nombrado en las investigaciones. Es muy activo en redes sociales con la temática del voto electrónico y uno de los primeros en publicar sobre las filtraciones que se investigan.

Siempre en cuanto interesa a esta presentación, señala el informe respecto de mi defendido:

Se obtuvieron las siguientes cuentas @mis2centavos (Twitter), www.facebook.com/javier.smaldone, @javier.smaldone (Instagram) y un

@blog.smaldone.com.ar (derivado del Facebook). Cabe señalar que Javier Smaldone en su información consta que vive en Córdoba y que su actividad laboral es programador. Asimismo, posteó en red social a Capitán_Alfa cuando este último refirió haber encontrado vulnerabilidades de un satélite con un amigo.

Hasta aquí, nuevamente información a todas luces intrascendente, y absolutamente nada que vincule al Sr. Smaldone con la investigación que refiere al seguimiento de los resultados de los datos que arrojaron los servidores vulnerados, ni mucho menos con la difusión de los datos ilegalmente obtenidos.

Luego, en el marco de un nuevo informe (fs. 432) puede verse —con preocupación— que mi defendido ha sido rigurosamente investigado.

Se dice:

Domicilio: ■■■■■■ ■■■ Rio Cuarto, Provincia de Córdoba.

Novedades: Se logró detectar movimiento dentro del recinto, observando una silueta masculina mirando por las rendijas de la persiana, motivo el cual se solicita información a la empresa prestataria del Servicio de Internet, diligenciar con la D.N.R.P.A. si posee vehículos a su nombre y la instalación de cámaras de vigilancia (resultado negativo). Asimismo, se informa que el investigado posee dos (2) hijos (que llevan su apellido) con la señora ■■■■■■■■■■■■■■■■■■■■, quien se domicilia en la calle ■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■ Ciudad de Rio Cuarto. Seguidamente, se hace mención que una de las señales Wi Fi próximas al domicilio investigado, podrían vincularse con el símbolo de los atacantes [S]. Asimismo se pudo determinar mediante tareas desplegadas en el domicilio de ■■■■■■■■■■, Rio Cuarto, que el Sr. Smaldone utilizaría un celular con el número 358------- y 358------- (este último de la ex mujer) ambos de la empresa Personal.

Asimismo mediante la utilización de Reporte de geolocalización se logró determinar a través del número 358------- que las antenas lo ubican en inmediaciones del Barrio de Recoleta, ■■■■■■■■■, diligencia practicada el 28/8/2019 horas 15.45, distante 200 metros aproximadamente del domicilio que registrara gretelcamos@gmail.com a través de Mercado Libre, en Av. Santa Fe 17■■, CABA, tratándose de un comercio donde no fue habido el

buscado ni es conocido, de la misma manera se realizaron nuevas tareas en inmediaciones y contándose con el domicilio de Santa Fe 16■■, donde según informe de Mercado Libre fueron entregados los celulares marca XIAOMI, se trata de un edificio de ocho pisos con dos departamentos por cada uno de ellos, donde no fue habido Smaldone ni es conocido; por lo cual y habiendo efectuado una nueva geolocalización la misma dio en ■■■■■■■ ■■■■■■■■■■, siendo vista una persona de similares características fisonómicas ingresar al domicilio de dicha arteria en la numeración ■■■■■, donde las tareas determinaron que allí vive sin poder certificarse que se trate del mismo. Por otro lado, se continuaron tareas en las inmediaciones y con fecha 11 de septiembre del corriente año se visualizó una pareja compuesta por una mujer y un hombre; surgiendo de las tareas en el lugar que se domicilian en la misma arteria pero en la numeración ■■■■, piso X departamento X, CABA, obteniéndose vista fotográfica y casi con exactitud se trataría de Javier Smaldone...

Sobre este informe, puedo decir que:

1.- No advierto de qué modo —la policía tampoco lo explica— una de las señales Wi Fi próximas al domicilio en Rio Cuarto podría vincularse con el símbolo de los atacantes [S]. Y tampoco tengo claro —la policía tampoco lo dice— qué podría significar ello a los fines de esta investigación.

2.- Las antenas telefónicas del celular de mi defendido lo ubican a 100 metros del domicilio donde se aloja cuando esta en esta Ciudad, en una de las zonas más densamente pobladas y con actividad comercial de la misma.

Luego, a fs. 488 luce un pedido de la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina que, por sus características, ya pone de manifiesto sin ambages la intención de avanzar sobre la intimidad del Sr. Smaldone con total independencia de la investigación en curso.

En este escenario, cuando todos los esfuerzos por vincular al nombrado con el caso fracasaron estrepitosamente, aparece un informe incalificable.

Puede verse a fs. 515 bajo el título: *Indicios que componen en su conjunto una sospecha fundada bajo los criterios de investigación policial respecto de la vinculación de Javier Smaldone con los hechos investigados.*

El informe está estructurado del siguiente modo:

<u>Análisis previo</u>:

1. *En el hecho investigado se ha publicado mediante la red oscura información confidencial de personal policial de la PFA. Dicha información fue obtenida mediante ataques informáticos a sistemas.*

<u>Indicios</u>:

1. *Indicio: Sindicación por parte de terceros.*
2. *Indicio: Intereses en común.*
3. *Indicio: Iniciativa en publicación (concepto de "quema controlada").*
4. *Indicio: Análisis temporal causa efecto (modo privado de la cuenta).*
5. *Indicio: Hostigamiento hacia el personal policial que investiga causas conexas.*
6. *Indicio: Aversión hacia la policía manifestada en forma pública.*
7. *Indicio: Publicación de análisis de casos investigados.*
8. *Indicio: Vinculación con actores de causas conexas.*
9. *Indicio: Análisis de información técnico-informático.*
10. *Indicio: Análisis de información geo-referencial temporal.*
11. *Indicio: Información obtenida mediante pedidos de informes.*

<u>Consideraciones</u>:

1. *Si bien la aclaración es redundante a las reglas de la propia disciplina de la investigación policial, se hace mención que los intereses el uso de herramientas o conocimientos técnicos específicos por si solos no son elementos que generen una sospecha fundada, pero analizados de forma íntegra, en un contexto determinado, con elementos concurrentes y concomitantes producen un cuerpo de análisis que nutre a la investigación y reducen incertidumbres. Es así que los análisis parciales o con falta de integridad respecto de este cuerpo de indicios no componen el presente análisis completo y carecen de integridad.*

El informe al cual me vengo refiriendo, plagado de reflexiones primitivas, es desopilante, un maltrato a la inteligencia, por las siguientes razones.

1) *Sindicación por parte de terceros*.

Aparentemente, un posteo dice: "*Smaldone strikes again (Hackearon a la PFA edition)"* y alguien twiteó "*Che Smaldone, deja de hackear sitios".*

2) *Intereses en común.*

Se observa intereses en común respecto de la información visualizada en el ataque con el perfil analizado: Voto electrónico, Pablo Tonelli, Patricia Bullrich (¿????). Esto significa que por criticar de manera pública y particularmente fundada una cuestión de máximo interés para todos los ciudadanos como lo es todo cuanto se vincula con nuestro proceso electoral, mi defendido tiene un interés común con quien vulnera la seguridad informática de la policía. Un médico ahí.

3) *Iniciativa en publicación (concepto de "quema controlada").*

Se visualizan diversas publicaciones donde Javier Smaldone hace referencia a ataques no se adjudica la autoría, pero da difusión de los mismos generando difusión de los daños generados. A la vez también se visualiza publicaciones en medios periodísticos donde da explicaciones de los mismos como "consultor" o "técnico" (¿????).

A esto, agrego yo, en los lugares civilizados se lo conoce como periodismo.

4) *Análisis temporal causa efecto (modo privado de la cuenta).*

En el marco de la investigación y donde se realizando diversas tareas Javier Smaldone bloquea la visualización a su cuenta actual de twitter (@mis2centavos), si bien se refiere a un hecho difundido en medios periodístico (https://www.abcdiario.com.ar/espectaculos/2019/8/26/alfredo-casero-exploto-contra-smaldone-que-panquequeada-pegaste-6984.html) a la vez coincide en los momentos de las tareas propias de la investigación (¿????).

Esta afirmación supone que mi defendido estaba al tanto de los contornos de la presente investigación, y justo —justo— cuando la policía intento visualizar su cuenta, el nombrado activó la función de proteger sus tweets. Como si de tal modo pudiese impedir el progreso de la investigación.

5) *Hostigamiento hacia el personal policial que investiga causas conexas.*

De forma constante y persistente se realizan hostigamientos hacia el personal policial que realizó tareas de investigación manifestando "besis, cabo Landajo" o "Y agarrate, vos, ayudante del cabo Landajo porque te voy a mandar al frente hasta con el color favorito de calzoncillos. Buche de cuarta". Dicho hostigamiento virtual constante y persistente también, es referenciado en su blog personal (¿????).

A todo evento, pongo en conocimiento del Tribunal que, más allá de enfrentar un hecho inédito en materia social, cuál es la policía quejándose de bullying, mi defendido mantiene una relación pública de tono crítico con dicha fuerza, desde la primera vez que se intentó vincularlo con una investigación criminal. La empezaron ellos.

6) *Aversión hacia la policía manifestada en forma pública.*

   De forma constante se manifiesta aversión hacia la policía (¿????).

7) *Publicación de análisis de casos investigados.*

   Se observa como realiza un análisis detallado de diversos casos obteniendo información de terceras partes (¿????). Mi defendido es especialista en seguridad informática, y se dedica a divulgar información de interés general sobre el tema, no solo en redes sociales sino también en su blog, en congresos especializados y en notas publicadas en medios masivos de comunicación. Nuevamente, en los lugares civilizados a esto se le llama periodismo.

8) *Vinculación con actores de causas conexas.*

   Se observan vinculaciones entre la cuenta analizada y otras cuentas como LIberoamericaMU, Capitan_Alfa, hispahack (¿????).

   Solo diré aquí que en sus más de nueve años de uso de la red social Twitter, con cierto protagonismo en su esfera de conocimiento y habiendo llegado a tener más de treinta y seis mil seguidores, el Sr. Smaldone mantuvo "vinculaciones" con muchísimos usuarios cuya actividad privada ciertamente desconoce.

9) *Análisis de información técnico-informático.*

   En los ataques se visualiza información técnica concordante con las descriptas por el actor tanto en la cuenta de Twitter como así en su CV (¿????).

Se sugiere aquí que por sus conocimientos, mi defendido se encuentra en condiciones de llevar adelante la maniobra investigada. El Sr. Smaldone –y olvidó la policía decir- miles de personas más, solo en nuestro país, que se interesan por la informática.

10) *Análisis de información geo-referencial temporal.*

Respecto de la información geo-referencial se aprecia lo siguiente: i) misma ubicación entre Emanuel Velez Cheratto y Javier Smaldone son de la Provincia de Córdoba, ii) Javier Smaldone realiza una visita a Santa Fe específicamente en la localidad de Santo Tomé, donde hay vinculaciones con diversas acciones en la referente causa (donde fue como observador electoral colaborando con la Fundación Poder Ciudadano, capitulo argentino de Transparency International). Dicha visita, se omite aclarar, ocurrió en el mes de abril de este año, iii) la contratación de Fulltech (Santa Fe 17■■) se declara en un domicilio cercano a la ubicación real de Javier Smaldone y iiii) Celulares XIAOMI se generan compras con domicilio de envío en Santa Fe 16■■, ubicación cercana a la ubicación real de Javier Smaldone, según información provista por Mercado Libre.

11) *Información obtenida mediante pedidos de informes.*

Según información analizada de los pedidos de informe a las empresas de telefonía celular, se observan similitudes respecto de los momentos de alta del VPS y solicitud de baja. Viendo que ambos cuentan con patrones similares de la señal de telefonía celular (¿????). Incomprensible.

Este informe muestra, en mi modo de ver las cosas, que la especie humana, tras siglos de civilización, sigue conservando rasgos bárbaros: en franco desconocimiento del arte de la fundamentación, la línea que separa lo real de lo imaginario aparece aquí un tanto difusa. Basta tener estudios elementales para advertir que mediante este informe se fuerzan, hasta el absurdo, argumentaciones carentes de todo sustento con el único fin de involucrar a mi defendido en el caso. Un método que se utilizaba hace muchos años para canalizar escarmientos.

En ausencia de un mínimo de consistencia intelectual, con estos métodos de investigación, no me sorprende que una investigación naufrague; me sorprende que llegue a puerto.

¿Para esto pagamos tantos impuestos?

Como en muchos informes policiales, lo de menos es lo que dice; lo único que tiene interés es lo que deja afuera: en el caso, el malestar que genera en ciertos ámbitos políticos las investigaciones desarrolladas por el Sr. Smaldone en tanto se vinculan con el voto electrónico.

Vuestra Señoría no tiene porqué saberlo, pero desde hace más de veinte años mi defendido participa públicamente, de manera activa, en distintos debates referidos a cuestiones de máximo interés público. En este último tiempo, ha tenido —dicho modestamente— una participación relevante en todo cuanto se vincula al sistema electoral, más concretamente a la introducción de herramientas informáticas en los procesos de votación y escrutinio, con fuertes críticas a la iniciativa del actual gobierno para la implementación del voto electrónico.

Por estas cuestiones expuso ante el plenario de comisiones de la Honorable Cámara de Diputados y dos veces ante el plenario de comisiones del Senado de la Nación.

Ello, además de haber publicado decenas de notas en diferentes medios de comunicación, de haber expuesto en diversos congresos y jornadas, y de haber participado de la elaboración de un libro sobre el tema.

Con base en este informe, con fecha 25 de setiembre pasado, la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina solicita de V.S. distintos procedimientos, entre ellos el allanamiento de un domicilio que mi defendido frecuenta, con el objeto de secuestrar telefonía celular, elementos informáticos, dispositivos de almacenamiento, anotaciones y registros vinculados a la maniobra investigada (fs. 533).

IV

Sobre la base de estos antecedentes, con fecha 3 de octubre pasado (fs.591) V.S. dispuso el allanamiento que aquí se cuestiona.

Como ha quedado acabadamente descripto, ni mediando un esfuerzo de imaginación superlativo puede sostenerse que existiese respecto del Sr. Smaldone, a los fines de disponer una orden de allanamiento en el domicilio donde se aloja cuando visita esta Ciudad, motivos, razones o fundamentos que surjan *legítimamente* ni del propio decisorio que aquí se cuestiona, ni de otra pieza procesal a la cual dicho auto remita en forma inequívoca, ni de constancia alguna arrimada al proceso con anterioridad al dictado del mismo, de la cual surja de forma indudable la necesidad de proceder.

En modo alguno puede siquiera sugerirse que una medida intrusiva de las características de la que aquí nos ocupa sea una derivación lógica de lo actuado hasta el momento, ni una consecuencia categórica de probanzas colectadas con antelación.

No se puede individualizar en todo el legajo un elemento que autorice lo dispuesto por el Tribunal. Así, la lectura de todo lo actuado no permite tener a la vista las motivaciones de la medida dispuesta, violatoria de disposiciones constitucionales que hacen a la protección del domicilio y de la intimidad de mi defendido.

[redacted]

No puedo pasar por alto que so pretexto de desarrollar una investigación que versa sobre cuestiones tecnológicas, se intentó obtener los datos correspondientes a la tarjeta SUBE y a la cuenta de *WhatsApp* de mi defendido, a la vez que se colocaron cámaras de vigilancia frente a la vivienda de sus hijos, aun en el conocimiento que aquel no se encontraba en el lugar.

Y que estas medidas solo se instrumentaron a su respecto: el resto de las personas involucradas en esta investigación tuvo mejor suerte.

Para disponer un allanamiento, el auto que lo ordena debe sustentarse en una base seria y suficiente para justificarlo. No basta el cúmulo de información **falsa, tergiversada** e **intrascendente** mediante la cual la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina llevó a engaño al Tribunal, formando su convicción acerca de la existencia de motivos legalmente válidos para fundar su proceder.

Por tal motivo, oportunamente se solicitó la declaración de nulidad del auto que ordena el allanamiento cuestionado, y en virtud lo normado en el artículo 172 del Código Procesal Penal de la Nación, la nulidad de todos los actos consecutivos que de él dependen, concretamente, el secuestro verificado en la ocasión.

V

En la misma dirección, se postuló el dictado de un sobreseimiento respecto de mi defendido, en la inteligencia que no existe el menor indicio —más allá de la imaginación policial— que sugiera que ha participado en la intrusión investigada, o en la difusión de la información así obtenida.

Las maniobras investigadas conllevan el peligro a la seguridad nacional que implica que información propia de las fuerzas de seguridad se encuentre en manos de particulares, que podrían afectar intereses de la República Argentina a partir de la revelación de secretos propios de la Policía Federal Argentina.

Por tal motivo, se dijo, no debía V.S. permitir que se desvíe el curso de la investigación correspondiente, con la evidente intención de vincular al proceso a personas que ninguna relación guardan con el mismo, y al amparo de una supuesta investigación dar amparo a seguimientos inadmisibles en el marco de un Estado de Derecho.

VI

Una vez formado el correspondiente incidente, V.S. corrió traslado a las partes de este expediente.

El Señor Fiscal interviniente en autos, Dr. Jorge Felipe Di Lello, sostuvo que nos encontramos en una etapa primaria de la investigación, motivo por el cual el hecho de adentrarse en el estudio de la cuestión tal como lo pretende esta defensa, no podrá darse sino por las aristas formales de la diligencia en cuestión, so pena de adelantar valoraciones propias de la otra etapa procesal.

Así, el titular de la acción penal dijo que la nulidad formulada intenta valorar los elementos que el instructor tuvo en consideración para el dictado de la medida cuestionada, acudiendo con una lectura diversa sobre la validez de las constancias policiales. Consideró que, a su criterio, la entidad de los

informes policiales y de las demás constancias se ven jaqueadas por apreciaciones que, a esta altura, parecen más de una discusión sobre el mérito de la prueba, más que el valor primario y reciente que tienen las definiciones del actuar previsional para fundamentar la diligencia cautelar.

Precisó el Dr. Di Lello que los elementos tenidos en cuenta para el allanamiento fueron resultado del estudio previo de las constancias recolectadas y también de la necesidad expresada por la prevención y ratificada luego por el Tribunal, de contar con elementos que permitieran continuar con la investigación, no surgiendo a su criterio que estuviera presenta la búsqueda de la responsabilidad de Smaldone, pues el nombrado no ha sido el único sindicado por los investigadores, ya que, de hecho, hay otros usuarios, por lo cual no aparece en escena el direccionamiento pesquisitivo hacia él, ni que la decisión judicial responda a otros intereses.

En el mismo sentido, el Representante de la Vindicta Pública estimó que de la lectura del decisorio de fs. 591/606, existe un relato respecto de Javier Smaldone que, prima facie, constituiría una situación que puede sustentar dicha diligencia, y así conocer las comunicaciones con aquéllos sospechados, como así también otros extremos que son necesarios corroborar y que solo con las computadoras o su celular pueden determinarse.

Sostuvo también el Señor Fiscal, que entiende y comparte la preocupación que Smaldone transmite con un claro mensaje de preservación de un bien tan preciado por la Constitución Nacional, como es la protección no solo del debido proceso legal sino de la inviolabilidad de las comunicaciones de los ciudadanos; sin embargo, el ataque a la validez formal de la diligencia en cuestión, no aparece como cuestionable desde donde se intenta, ya que la mera invocación de presentar circunstancias violatorias de derechos, van más allá de dichas garantías, al formar la diligencia aludida una parte de la decisión que involucra a varios usuarios, y que la utilización de distintas comunicaciones y demás constancias probatorias, solo con la información directa puede comenzarse un autentico estudio técnico.

Destacó el Dr. Di Lello que los derechos no terminan allí, sino que el control de la legalidad surge después del secuestro y, a su criterio, ésta no es una prueba que se incorpora al sumario por si, sino que exige una revisión formal y un análisis que extreme los elementos requeridos por el Tribunal, sin

sobrepasar tal marco, donde el actuar autorizado no puede resultar atentatorio de sus derechos. Esa es la razón, sostuvo, por la que tomar una decisión sobre la incorporación de la prueba, más en el caso de computadoras o celulares, debe ir acompañada de un examen técnico que satisfaga no solo a la instrucción sino también a los derechos aludidos y por los que esta parte hoy reclama su reconocimiento, aún a través de una vía que no se comparte como solución procesal.

Por último, consideró que responder a todos y cada uno de los puntos introducidos en la nulidad importaría habilitar la discusión de la prueba en forma temprana, cuando será la instrucción del sumario donde haya tiempo para revisarla, sin dejar de señalar el titular de la acción penal que los elementos que sirvieron de base para sustentar el registro domiciliario cuestionado, serán materia de análisis a lo largo de la pesquisa y no pueden ser forzados en su entidad probatoria con la sola disconformidad o interpretación del incidentista.

De tal modo, el Señor Fiscal estimó que no puede tener acogida favorable la nulidad introducida.

VII

Los argumentos vertidos por el Fiscal, receptados por el Tribunal al resolver el planteo que aquí nos ocupa, son sencillamente inaceptables.

Sin dejar de señalar que algunos párrafos que integran el dictamen del Ministerio Público Fiscal me resultan incomprensibles, por su vaguedad o ausencia de alguna conceptualización en concreto, quiero señalar mi profundo disenso con todo cuanto allí se expone.

Así, esta parte no advierte, ni el señor Fiscal tampoco lo explica, cual es la relevancia a los fines de resolver el planteo que da origen a esta incidencia el hecho de que nos encontremos en una etapa primaria de la investigación.

Tampoco se advierte por qué motivo al resolver un planteo de nulidad se adelantan valoraciones propias de la otra etapa procesal.

Así, el titular de la acción penal señaló que la nulidad formulada intenta valorar los elementos que el instructor tuvo en consideración para el dictado de la medida cuestionada, acudiendo con una lectura diversa sobre la validez de las constancias policiales. Y este es un error de concepto inconcebible, en

tanto esta parte señaló y demostró racionalmente que los elementos que se valoraron al dictar la medida cuestionada son falsos, y deben analizarse en el contexto de una persecución judicial impropia de un estado de derecho.

Lo que omite decir en su dictamen el Dr. Di Lello es que los elementos tenidos en cuenta para el allanamiento cuestionado fueron irregularmente concebidos por la policía, y no el resultado del estudio previo de las constancias recolectadas, y que la necesidad expresada por la prevención y ratificada luego por el Tribunal, de contar con elementos que permitieran continuar con la investigación no hace sino consentir el progreso de una actividad instructoria cimentada sobre una base ilegal, y que no tiene por objeto alcanzar la verdad, ni nada parecido.

No hemos dicho que Smaldone ha sido el único sospechoso sindicado por los investigadores. Hemos dicho que mi defendido ha sido traído a este proceso sobre la base de mentiras que han quedado probadas en el legajo más allá de cualquier duda que pudiese existir.

En el mismo sentido, cuando el Representante de la Vindicta Pública estima que de la lectura del decisorio de fs. 591/606, existe un relato respecto de Javier Smaldone que, prima facie, constituiría una situación que puede sustentar dicha diligencia, omite decir que se trata de un relato falso, construido sobre probanzas tergiversadas de un modo legalmente inaceptable.

Se agradece al Señor Fiscal que entienda y comparta la preocupación que el Sr. Smaldone transmite con un claro mensaje de preservación de un bien tan preciado por la Constitución Nacional, como es la protección no solo del debido proceso legal sino de la inviolabilidad de las comunicaciones de los ciudadanos; sin embargo, no explica el Dr. Di Lello por qué razón considera que “el ataque a la validez formal de la diligencia en cuestión, no aparece como cuestionable desde donde se intenta, ya que la mera invocación de presentar circunstancias violatorias de derechos, van más allá de dichas garantías, al formar la diligencia aludida una parte de la decisión que involucra a varios usuarios, y que la utilización de distintas comunicaciones y demás constancias probatorias, solo con la información directa puede comenzarse un autentico estudio técnico”.

Por lo demás, al sugerir que tomar una decisión sobre la incorporación de la prueba, más en el caso de computadoras o celulares, debe ir acompañada de un examen técnico que satisfaga no solo a la instrucción sino también a los derechos aludidos y por los que esta parte hoy reclama su reconocimiento, aún a través de una vía que no se comparte como solución procesal, deja en claro que el Ministerio Público no ha comprendido en absoluto el planteo que nos ocupa.

Pareciera ser, por lo menos así lo entiendo yo, que el fiscal quiere examinar los elementos secuestrados y luego ver si los incorpora como prueba o no. Y esta parte ha sido muy clara: no existían razones —en lo más mínimo— que autorizasen conforme a derecho los secuestros cuestionados.

Por lo demás, y en términos docentes, es una pena que el Fiscal no diga las razones por las cuales le parece que la vía intentada (un planteo de nulidad) no resulta idónea para canalizar un planteo de nulidad.

Por último, y esto es insólito, el Ministerio Público consideró que responder a todos y cada uno de los puntos introducidos en la nulidad importaría habilitar la discusión de la prueba en forma temprana, cuando será la instrucción del sumario donde haya tiempo para revisarla, sin dejar de señalar que los elementos que sirvieron de base para sustentar el registro domiciliario cuestionado, serán materia de análisis a lo largo de la pesquisa y no pueden ser forzados en su entidad probatoria con la sola disconformidad o interpretación del incidentista.

Una vez más: el momento de revisar la prueba —en tanto se alude a los elementos que sirvieron de fundamento a una orden de allanamiento y secuestro— es ahora. El Código Procesal Penal de la Nación es clarísimo al respecto.

Y evidentemente el Dr. Di Lello no ha leído en profundidad nuestro planteo, que no trasluce una disconformidad o diferente interpretación de la entidad probatoria de los elementos que sirvieron de base para sustentar el registro domiciliario cuestionado, sino que ha denunciado una maniobra inaceptable del personal que colaboró con la instrucción que tuvo por objeto vincular de un modo irregular a una persona a un caso del que resulta totalmente ajeno, mintiendo para ello descaradamente.

Al momento de resolver la cuestión, V.S. consideró que el planteo nulificante efectuado esta defensa no puede prosperar, en tanto no se evidencia la violación a la garantía constitucional de defensa en juicio y debido proceso alegada.

Al respecto, señaló que la medida dictada por quien suscribe, —no solo respecto del incidentista sino respecto de otros catorce domicilios en diversos distritos de la República, tal como surge del auto de fs. 591/606 de los autos principales— se encontró orientada a recabar mayor información en orden a la posibilidad de intensificar la investigación y a los fines de contrastar, efectivamente, las hipótesis desarrolladas por el personal policial —al menos, con las probanzas y análisis glosados a fs. 93/94, 224/231, 240/241, 433/435, 440/441, 515/532, 544 de los autos principales y a fs. 113, 1157/1160, 675/690 del legajo de prueba formado en autos—, con el material electrónico y de comunicaciones que pudiera encontrase en poder de los individuos sospechados, de los cuales llegose incluso a reclamar el cercenamiento de sus libertades ambulatorias.

Una vez más, se argumenta respecto de cuestiones no planteadas, y se exhiben razones intrascendentes a los fines de resolver el presente planteo.

Es obvio, no existe la menor duda que la medida cuestionada se encontró orientada a recabar mayor información en orden a la posibilidad de intensificar la investigación y a los fines de contrastar, efectivamente, las hipótesis desarrolladas por el personal policial. Lo que esta parte ha planteado es que no existían razones para recabar información en el domicilio del Sr. Smaldone, y que la policía engañó a ese respecto al Tribunal, con elementos falsos.

En consonancia con el parecer expuesto por el Sr. Representante del Ministerio Público Fiscal, V.S. estimó que el cuestionamiento formulado por la defensa no expresa de qué forma le ha sido conculcada la garantía en cuestión, ni tampoco se advierte un perjuicio real y concreto que permita hacer viable el remedio inmediato.

En tal sentido, V.S. invocó un precedente de la Sala II de la Excma. Cámara del Fuero que ha dicho que “Solo cabe anular las actuaciones cuando el vicio afecte un derecho o interés legítimo y cause un perjuicio irreparable, sin admitirlas cuando no exista una finalidad práctica, que es razón ineludible

de su procedencia”. (Cattani- Irurzun- Farah, CCCfed. Sala IIa., causa nro. 27.130 “Boyko, Daniel P. s/ nulidad”, rta. El 23/09/08, reg. Nro. 28.954).

Pareciera ser que el Tribunal no ha advertido en lo esencial cuanto se desprende de la cita escogida, puesto que si ese fuera el caso, dicho precedente no hace otra cosa que dar razón —de manera contundente— a esta defensa.

Así, V.S. ha compartido la línea argumentativa desarrollada por el Ministerio Público —ya rebatida en este escrito—, y en especial rescata una idea elemental e intrascendente, cual es que es justamente la finalidad y meta principal de esta etapa preparatoria construir el objeto del proceso mediante su avance. De tal modo, mediante el desarrollo de esta actividad se irá edificando, progresivamente, el objeto de este legajo, radicando allí la naturaleza de la instrucción. Pues, efectivamente, es durante ella donde se tiende a precisar la imputación, que durante su desenvolvimiento es fluida y puede experimentar modificaciones y precisiones; de allí que durante este procedimiento el objeto resulta construido y es modificable, hasta quedar fijo en la acusación o, en su caso, cuando se la descarta.

Si, claro.

Pero nada de ello puede hacerse violentando garantías constitucionales.

Analizar el informe policial que motiva el allanamiento cuestionado, tanto para el fiscal como para V.S. es algo que no corresponde a esta etapa procesal. Y no puedo más que estar de acuerdo en eso. La diferencia entre mi criterio y el vuestro es que la valoración de estos supuestos indicios que sustentaron la medida que aquí se cuestiona debió haberse hecho antes de autorizar la violación de la intimidad de mi defendido y su pareja y de privarlos de sus herramientas de trabajo y su información personal y profesional.

Luego de exteriorizar una serie de abstracciones cuya relación con este caso no se advierte, no puede dejar de verse que ni V.S. ni el fiscal fueron capaces de señalar un solo elemento que justifique el allanamiento puesto en crisis.

Y sorprende que nadie perciba ninguna violación de derechos, ni tampoco ningún daño.

Se ignora en el caso el respeto por elementales garantías constitucionales, en particular las que refieren a la inviolabilidad del domicilio y de la correspondencia privada, además del secreto de las fuentes de información periodística (tal el contenido de algunos de los dispositivos que fueron secuestrados).

Más de 35 organizaciones no gubernamentales y grupos de la sociedad civil de 10 países, incluyendo al Consejo Directivo de una Facultad de una Universidad Nacional argentina, se han pronunciado alarmados por la flagrante violación de los derechos del Sr. Smaldone y el peligroso precedente que sientan las medidas adoptadas hasta ahora por la Justicia. El presente caso fue tratado en el Foro de la Gobernanza de Internet realizado en Berlín el pasado mes de noviembre, como un ejemplo de persecución política a activistas de los derechos digitales. Entre las organizaciones que se han expresado preocupadas por esta situación, avalando la posición de esta parte, se encuentran algunas tan prestigiosas como Poder Ciudadano y el Centro de Estudios Legales y Sociales —a nivel local— y Amnistía Internacional, Human Rights Watch, Reporteros Sin Fronteras y la Electronic Frontier Foundation —a nivel internacional.

Curioso es también que nadie perciba un daño concreto hacia mi defendido. Las fuerzas policiales violaron la intimidad de su domicilio, le quitaron sus herramientas de trabajo y sus datos (dificultando o imposibilitando su actividad laboral, y dañando a sus hijos, ambos estudiantes universitarios a su exclusivo cargo). Y esto además del tiempo insumido por los trámites legales y otras dificultades de índole psicológico (habiendo sido allanado y esposado sin haber hecho absolutamente nada, y viendo que en el expediente no hay ningún elemento real que justifique semejantes medidas, ¿cómo puede estar seguro de conservar su libertad, o de no ser visitado nuevamente por la policía?). El daño concreto, que se intenta evitar con este pedido de nulidad del allanamiento, es la violación de

su correspondencia, de información de índole privada, y de información confidencial de naturaleza periodística (amparada en el derecho constitucional de protección de las fuentes).

Recuerdo nuevamente, para finalizar, que en los dispositivos secuestrados se encuentra material confidencial de investigaciones periodísticas finalizadas (que han sido publicadas) y otras que se encuentran en curso, incluyendo tanto información confidencial como así también diálogos del Sr. Smaldone con varios periodistas argentinos y extranjeros.

VIII

En virtud de lo dicho, ante la eventualidad de una solución adversa a la que se propone, formulo la protesta de casación y la reserva del caso federal en razón de los agravios constitucionales señalados en este escrito.

IX

En virtud de todo lo expuesto, habré de solicitar de V.S. que conceda el presente recurso de apelación, interpuesto en legal tiempo y forma, y eleve todo lo actuado a conocimiento del Superior, a los fines que resuelva en definitiva.

Tener presente lo expuesto,

SERÁ JUSTICIA

UNC Universidad Nacional de Córdoba
FAMAF Facultad de Matemática, Astronomía, Física y Computación

EL CONSEJO DIRECTIVO
DE LA FACULTAD DE MATEMÁTICA, ASTRONOMÍA, FÍSICA Y COMPUTACIÓN

DECLARA:

Que ante la inquietud expresada por un grupo significativo de docentes de nuestra institución frente a los hechos de público conocimiento que afectaron recientemente al experto en informática Javier SMALDONE, este cuerpo manifiesta su preocupación.

El señor SMALDONE es un referente nacional en la oposición al voto electrónico y ha protagonizado conocidas controversias sobre el tema con el actual Poder Ejecutivo Nacional.

Como en otras situaciones similares este cuerpo quiere ratificar su profunda convicción de que nuestras instituciones deben velar por la plena vigencia del estado de derecho y el cumplimiento de las garantías constitucionales.

DADA EN LA SALA DE SESIONES DEL CONSEJO DIRECTIVO DE LA FACULTAD DE MATEMÁTICA, ASTRONOMÍA, FÍSICA Y COMPUTACIÓN A LOS ONCE DÍAS DEL MES DE NOVIEMBRE DE DOS MIL DIECINUEVE

DECLARACIÓN CD N.º 6/2019

Dra. SILVIA PATRICIA SILVETTI
SECRETARIA GENERAL
FaMAF

Dra. Ing. MIRTA IRIONDO
DECANA
FaMAF

INTERPONE RECURSO DE CASACIÓN.RESERVAS.

Excma. Cámara:

Pablo Slonimsqui, abogado defensor del Sr. Javier Lorenzo Carlos Smaldone, en la causa que lleva el nº 55276/2019 del registro de la Secretaría nº 18 del Juzgado Nacional en lo Criminal y Correccional Federal nº 9 –**Incidente nº 3**-, manteniendo el domicilio constituido en el Pasaje Rodolfo Rivarola 193, piso 3º oficina 11 de esta Ciudad Autónoma de Buenos Aires, ante V.E. me presento y digo:

I

Que vengo por intermedio del presente, en legal tiempo y forma, y conforme expresamente lo autoriza la normativa procesal vigente, a interponer el correspondiente recurso de casación en contra de lo resuelto por el Tribunal con fecha 14 de febrero pasado, en tanto confirma la resolución oportunamente dictada por el titular del Juzgado Nacional en lo Criminal y Correccional Federal nº 9, quien dispuso rechazar el planteo de nulidad interpuesto por esta parte.

Dicha resolución, por sus características, causa a esta parte un gravamen irreparable.

Ello así, conforme los argumentos de hecho y de derecho que seguidamente expondré.

II

En el concepto de esta parte, el recurso de casación que se interpone resulta procedente.

Así. Puesto que si bien en principio el pronunciamiento criticado no reúne las características exigidas por el ordenamiento ritual para accede a la vía invocada, lo cierto es que el tenor de las críticas introducidas exige apartarse de esas restricciones legales.

De seguido, se verán los motivos por los cuales ese resolutorio, no definitivo en la noción del legislador, debe comprenderse como de naturaleza equiparable.

Los perjuicios de imposible reparación ulterior que es capaz de conllevar la postergación en el tratamiento de la materia debatida, dados los derechos que en ella se disputan, exigen que su atención eluda los estrictos alcances a los que refieren las palabras de la ley.

En efecto, esta defensa ha demostrado a lo largo de la actividad desarrollada en esta incidencia, un claro compromiso de garantías individuales básicas a partir de los actos cuyas nulidad peticiona.

Ello así, en la medida en que tanto la decisión del juez a quo como la da esta Cámara supone la conservación de esas medidas probatorias oportunamente impugnadas, la lesión de los derechos constitucionales del imputado se mantiene aun vigente, del mismo modo en que también lo hace la necesidad de una respuesta que los tutele. A ella es que se proyecta la herramienta procesal intentada y cuya prosperidad, frente al panorama señalado, no puede verse obstaculizada por una limitación que desconozca los altos valores involucrados.

De esta forma, ante un gravamen que, en esencia, no supone sino una genuina cuestión federal, es que corresponde a la Cámara Federal de Casación Penal intervenir en la contienda como órgano jurisdiccional intermedio al Máximo Tribunal.

En consecuencia, toda vez que este recurso satisface el cumplimiento de los demás requisitos establecidos en el código de forma –en orden al tiempo y forma del recurso-, a la vez que especifica las razones por las que se discrepa con la opinión de este Tribunal, indicando y analizando cada uno de los puntos sometidos a controversia, esta parte entiende que el mismo resulta procedente.

En este punto, cabe también señalar que enfrentamos un caso de arbitrariedad y de gravedad institucional, en la medida en que se evidencia en forma incontrastable que lo resuelto desatiende las reglas de la lógica, la experiencia general y el recto entendimiento, y proyecta un precedente nefastos para cualquier habitante de nuestro país.

III

Se iniciaron las presentes actuaciones con fecha 30 de julio pasado, cuando la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina puso en conocimiento de la justicia los episodios que conforman el objeto procesal de estos actuados.

Así, conforme se desprende del testimonio de Claudio Ricardo Ramos, Subcomisario con funciones en la dependencia señalada, quien refirió que el 29 de julio pasado se recibió en varias dependencias de la Policía Federal un correo electrónico que simulaba provenir de la Superintendencia de Bienestar, el cual contenía un link que al ser accionado re-direccionaría a un formulario el cual solicitaba se completen datos personales y demás información.

Se trata de una maniobra conocida como *Phishing* y permite sustraer datos.

Luego, a través del Ministerio de Seguridad de la Nación, se tomó conocimiento que en la red social Twiter un usuario @lagorraleaks refirió haber subido a la Deep Web información relacionada con la Policía Federal, específicamente de las áreas de bienestar y drogas peligrosas, razón por la cual se supone que la información allí publicada puede ser la obtenida a través del mecanismo antes descripto.

La Deep Web, se aclara, es un área de internet sin control por parte de las empresas internacionalmente conocidas como Google y donde resulta muy difícil rastrear a los usuarios e información que allí se vuelca.

A partir de las alertas emitidas por la empresa Gmail se pudieron individualizar dos IPs que se corresponderían con las conexiones utilizadas por la persona que habría obtenido los datos de forma engañosa tras ingresar en la cuenta oficial de la Policía Federal sin autorización.

Y, siempre en el concepto del Subcomisario Ramos, teniendo en cuenta la modalidad y tipografía utilizadas por el usuario de Twitter @lagorraleaks2.0, a este hecho se lo puede relacionar con las personas que en el año 2017 hackearon la cuenta de la Ministra Patricia Bullrich.

Sobre esta base, se dio curso a una investigación tendiente a individualizar a los autores del hecho –cuya gravedad no solo nadie discute, sino que incluso mi defendido puso de manifiesto públicamente a través de su cuenta de Twitter inmediatamente de conocidos los acontecimientos-, investigación que muestra como dato significativo, de un modo evidente, manifiesto, notorio y ostensible, la intención de vincular al Sr. Smaldone con estos episodios, aun cuando para ello haya que recurrir a métodos que resultan particularmente infantiles.

IV

Puede verse de lo actuado que, a la par de una investigación racional, estructurada sobre elementos objetivos de análisis, mediando una creatividad de dimensiones modestísimas se pretendió ubicar a mi defendido como responsable de algo, de cualquier cosa, vinculado con los hechos investigados, aun cuando surge nítido del legajo su total ajenidad respecto de los mismos.

Y digo así, puesto que habiendo compulsado las actuaciones –por momentos con profundo asombro-, no solo no se advierte qué elemento probatorio podría eventualmente sustentar una imputación en contra del Sr. Smaldone, sino que tampoco se advierte en concreto –ni en abstracto- cuál sería el hecho que se le imputa.

A fs. 67/68 puede verse un informe remitido al Tribunal por la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina, donde se refieren las medidas de investigación realizadas sobre las máquinas de las dependencias policiales vulneradas, y se da cuenta de los progresos de la investigación estructurados a partir de dicho análisis.

Nada que decir sobre ello.

Pero el problema empieza cuando en dicho informe se anuncia que *teniendo en cuenta la posibilidad de que el autor de la maniobra pueda involucrar mayor cantidad de información y hacerla pública, es que personal nuestro se halla avocado* (sic) *a la observación de fuentes*

abiertas y redes sociales, detectando ciertos usuarios que habrían replicado la publicación en distintas redes sociales y sistemas de chat con la vulnerabilidad investigada.

Y sigue el informe:

En otro orden de cosas se destaca que esta División llevó a cabo las investigaciones en torno a los hechos suscitados en el año 2017, relacionado al acceso a la cuenta particular de red social Twitter de la Ministra de Seguridad de la Nación generada con el mismo modus operandi investigado en este caso, teniendo en cuenta la existencia actual del usuario de la red social TWITTER denominado @Lagorraleaks2.0, que no solo hace público los datos obtenidos de las dependencias afectadas de esta Policía Federal, sino que también se atribuye los hechos ocurridos en el año 2017 de la siguiente manera: "En enero del 2017 conseguí acceso a varios correos electrónicos del Ministerio de Seguridad, uno de ellos fue el de la actual ministra de seguridad, Patricia Bullrich, a través del cual tomé su cuenta en twitter. Meses más tarde publiqué los emails de varias fuerzas, que se conoció como "lagorraleaks". Defacee la web del ejército (o fue ISIS?), gendarmería, policía de la ciudad y hackee al diputado tonelli"

Ante esta situación, habiéndose comprobado la autoría de los autores involucrados en el hecho del hackeo a la cuenta de Twitter de la Ministra en el año 2017, y la capacidad técnica que estos presentan para llevar a cabo los presentes hechos, y habiendo encontrado publicaciones donde se adjudican estos al mismo tiempo, se considera a estos como posibles responsables del hecho, tratándose de las siguientes personas:

…

…

Javier Smaldone

Este informe es sencillamente escandaloso por una razón elemental: en ningún momento mi defendido ha sido imputado por la justicia por el hackeo a la cuenta Twitter de la Ministra de la Nación, circunstancia que puede verificarse mediante la compulsa de las actuaciones

correspondientes, que llevan el nº 1033/17 del registro del Juzgado Nacional en lo Criminal y Correccional Federal nº 2, Secretaria nº 4.

Por lo demás, esta defensa acompañó en las presentes actuaciones aquellas constancias que aclaran la cuestión sin margen para las dudas: en dicho legajo el Sr. Smaldone se presentó espontáneamente, se le recibió declaración testimonial, acompañó toda la información que consideró útil y pertinente para dicha investigación y colaboró con la justicia en todo cuanto estuvo a su alcance.

Oportunamente, se dijo, se adjunto copia de dicha declaración a estos actuados.

Por tal motivo, en la evidencia que se ha incorporado a este expediente un informe que contiene información objetivamente falsa, y que a la postre permitió que progresara una insólita imputación en contra del Sr. Smaldone, esta parte solicitó que sin perjuicio del trámite de las presentes actuaciones, se extraigan testimonios y se formule la denuncia correspondiente a los fines de investigar las razones que motivaron la presentación referida y la identidad de los ideólogos de tan patética estrategia.

Ello, teniendo en especial consideración que a partir de la incorporación de datos mentirosos en un expediente judicial (la policía se permitió el lujo táctico de inventar cosas) se desarrolló una investigación sobre la persona de mi defendido –desproporcionada en si misma, y de una intensidad muy superior a la que se verificó respecto del resto de los imputados- inadmisible en un estado democrático, cuyas verdaderas motivaciones exceden, por mucho, la declamada necesidad de investigar los hechos que integran esta causa.

Como se dijo oportunamente, se han intentado múltiples alternativas para incriminar al Sr. Smaldone, ninguna con éxito.

Y alguien debería responder por semejante atropello.

Retomando el curso de este legajo, podemos ver que a fs. 93/4 obra nuevamente dicho informe de la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina.

Luego, en el marco de un extenso informe se da cuenta que el ciberpatrullaje sobre la cuenta @mis2centavos no presenta datos de interés (fs.221) y que se detectó que un grupo creado dentro de la red social Telegram llamado “La gorra Leaks Team” y “Lagorraleaks 2.0”, comparte twetts de @mis2centavos en temas relacionados a “las elecciones 19”.

Menciones de la cuenta de mi defendido cuya vinculación con estos actuados no se alcanza a comprender pueden verse a fs. 224/vta., 225, 225, 227 y 231. Se trata, en lo esencial, de opiniones políticas y conceptos técnicos que interesan a quienes se dedican a la informática.

Llegamos así al informe obrante a fs. 236/43, mediante el cual la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina repasa los antecedentes de su tarea en el caso, y en cuanto aquí interesa señala que:

Por todo lo expuesto, hasta el momento se puede confirmar a prima face (sic) *dos tipos de acciones delictivas hacia las instituciones y funcionarios públicos.*

Uno de los ataques es la realizada a la seguridad informática de la Policía Federal Argentina (en el caso que nos ocupa), Prefectura Naval Argentina y a la Policía de la Ciudad, la cual dejó vulnerable la Seguridad Nacional ante los ciudadanos.

El segundo ataque se realizó con la utilización de las distintas redes sociales, portales públicos, plataformas de la web, etc; publicaciones que no solo dejan al descubierto documentos y/o datos sensibles y privados, sino que fomentan en sus comentarios e instigan a un accionar ciudadano contra las instituciones y funcionarios del Estado Nacional y de las Fuerzas Armadas y de Seguridad.

Es por ello, que el presente hecho delictivo derivó en 2 (dos) líneas principales de investigación: una el seguimiento de los resultados de los datos que arrojaron los servidores vulnerados y la otra línea investigativa sobre el monitoreo/análisis de las publicaciones por el atacante informático, como así también sobre otras publicaciones que puedan relacionarse a las mismas (posteos, comentarios, retwitteos, compartimiento de enlaces, etc).

Expresado el hecho, se observó en las publicaciones del atacante una posible relación con el hackeo efectuado a la Sra. Ministra de Seguridad de la Nación, en el año 2017, en virtud que la intromisión al correo de la Sra. Ministra fue realizada en dicho año por quien se autodenominada "La Gorra Leaks", ilícito investigado por la Policía Federal Argentina, específicamente por la División Delitos Tecnológicos del Departamento CIBERCRIMEN, que era comandado por el Comisario Víctor Chanenko, quienes eran los encargados de la investigación en 2017 y a los que se mencionan despectivamente en las publicaciones que nos ocupan.

Atento a ello, como dato de interés se vinculó a la investigación las personas que posiblemente tuvieron alguna relación con el hecho investigado en el año 2017, procediéndose a realizar búsquedas de publicaciones de los mismos en los distintos portales de fuentes abiertas y/o redes sociales, a fin de poseer algún dato de interés a la causa, siendo las personas a considerar:

…

…

Javier Smaldone (el cual utiliza la cuenta @misdoscentavos). El mismo se presentó en su momento en la causa del año 2017 (hackeo a la Ministra de Seguridad) al enterarse nombrado en las investigaciones. Es muy activo en redes sociales con la temática del voto electrónico y uno de los primeros en publicar sobre las filtraciones que se investigan.

Siempre en cuanto interesa a esta presentación, señala el informerespect de mi defendido:

Se obtuvieron las siguientes cuentas @mis2centavos (Twitter), www.facebook.com/javier.smaldone, @javier.smaldone (Instagram) y un @blog.smaldone.com.ar (derivado del Facebook). Cabe señalar que Javier Smaldone en su información consta que vive en Córdoba y que su actividad laboral es programador. Asimismo, posteó en red social a Capitán_Alfa cuando este último refirió haber encontrado vulnerabilidades de un satélite con un amigo.

Hasta aquí, nuevamente información a todas luces intrascendente, y absolutamente nada que vincule al Sr. Smaldone con la investigación que refiere al seguimiento de los resultados de los datos que arrojaron los servidores vulnerados, ni mucho menos con la difusión de los datos ilegalmente obtenidos.

Luego, en el marco de un nuevo informe (fs. 432) puede verse –con preocupación- que mi defendido ha sido rigurosamente investigado.

Se dice:

Domicilio: Rivadavia XXX, Rio Cuarto, Provincia de Córdoba.

Novedades: Se logró detectar movimiento dentro del recinto, observando una silueta masculina mirando por las rendijas de la persiana, motivo el cual se solicita información a la empresa prestataria del Servicio de Internet, diligenciar con la D.N.R.P.A. si posee vehículos a su nombre y la instalación de cámaras de vigilancia (resultado negativo). Asimismo, se informa que el investigado posee dos (2) hijos (que llevan su apellido) con la señora XXXXXXXXXXX, quien se domicilia en la calle XXXXXXXXX, Ciudad de Rio Cuarto. Seguidamente, se hace mención que una de las señales Wi Fi próximas al domicilio investigado, podrían vincularse con el símbolo de los atacantes [S]. Asimismo se pudo determinar mediante tareas desplegadas en el domicilio de Rivadavia XXX, Rio Cuarto, que el Sr. Smaldone utilizaría un celular con el número 358------- y 358------- (este último de la ex mujer) ambos de la empresa Personal.

Asimismo mediante la utilización de Reporte de geolocalización se logró determinar a través del número 358------- que las antenas lo ubican en inmediaciones del Barrio de Recoleta, XXXXX y XXXXX, diligencia practicada el 28/8/2019 horas 15.45, distante 200 metros aproximadamente del domicilio que registrara gretelcamos@gmail.com a través de Mercado Libre, en Av. Santa Fe 1748, CABA, tratándose de un comercio donde no fue habido el buscado ni es conocido, de la misma manera se realizaron nuevas tareas en inmediaciones y contándose con el domicilio de Santa Fe 1635, donde según informe de Mercado Libre fueron entregados los celulares marca XIAOMI, se trata de un edificio de ocho pisos con dos departamentos por

cada uno de ellos, donde no fue habido Smaldone ni es conocido; por lo cual y habiendo efectuado una nueva geolocalización la misma dio en Rodriguez Peña XXX, siendo vista una persona de similares características fisonómicas ingresar al domicilio de dicha arteria en la numeración XXX, donde las tareas determinaron que allí vive sin poder certificarse que se trate del mismo. Por otro lado, se continuaron tareas en las inmediaciones y con fecha 11 de septiembre del corriente año se visualizó una pareja compuesta por una mujer y un hombre; surgiendo de las tareas en el lugar que se domicilian en la misma arteria pero en la numeración XXX, piso X departamento X, CABA, obteniéndose vista fotográfica y casi con exactitud se trataría de Javier Smaldone…

Sobre este informe, puedo decir que:

1.- No advierto de qué modo –la policía tampoco lo explica- una de las señales Wi Fi próximas al domicilio en Rio Cuarto podría vincularse con el símbolo de los atacantes [S]. Y tampoco tengo claro –la policía tampoco lo dice- que podría significar ello a los fines de esta investigación.

2.- Las antenas telefónicas del celular de mi defendido lo ubican a 100 metros del domicilio donde se aloja cuando esta en esta Ciudad, en una de las zonas más densamente pobladas y con actividad comercial de la misma.

Luego, a fs. 488 luce un pedido de la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina que, por sus características, ya pone de manifiesto sin ambages la intención de avanzar sobre la intimidad del Sr. Smaldone con total independencia de la investigación en curso.

En este escenario, cuando todos los esfuerzos por vincular al nombrado con el caso fracasaron estrepitosamente, aparece un informe incalificable.

Puede verse a fs. 515 bajo el título: *Indicios que componen en su conjunto una sospecha fundada bajo los criterios de investigación policial respecto de la vinculación de Javier Smaldone con los hechos investigados.*

El informe está estructurado del siguiente modo:

Análisis previo:

1. En el hecho investigado se ha publicado mediante la red oscura información confidencial de personal policial de la PFA. Dicha información fue obtenida mediante ataques informáticos a sistemas.

Indicios:

1. Indicio: Sindicación por parte de terceros.
2. Indicio: Intereses en común.
3. Indicio: Iniciativa en publicación (concepto de “quema controlada”).
4. Indicio: Análisis temporal causa efecto (modo privado de la cuenta).
5. Indicio: Hostigamiento hacia el personal policial que investiga causas conexas.
6. Indicio: Aversión hacia la policía manifestada en forma pública.
7. Indicio: Publicación de análisis de casos investigados.
8. Indicio: Vinculación con actores de causas conexas.
9. Indicio: Análisis de información técnico-informático.
10. Indicio: Análisis de información geo-referencial temporal.
11. Indicio: Información obtenida mediante pedidos de informes.

Consideraciones.

1. Si bien la aclaración es redundante a las reglas de la propia disciplina de la investigación policial, se hace mención que los intereses el uso de herramientas o conocimientos técnicos específicos por si solos no son elementos que generen una sospecha fundada, pero analizados de forma íntegra, en un contexto determinado, con

elementos concurrentes y concomitantes producen un cuerpo de análisis que nutre a la investigación y reducen incertidumbres. Es así que los análisis parciales o con falta de integridad respecto de este cuerpo de indicios no componen el presente análisis completo y carecen de integridad.

El informe al cual me vengo refiriendo, plagado de reflexiones primitivas, es desopilante, un maltrato a la inteligencia, por las siguientes razones.

1) Sindicación por parte de terceros.

   Aparentemente, un posteo dice: *Smaldone strikes again (Hackearon a la PFA edition)* y alguien twiteó *Che Smaldone, deja de hackear sitios.*

2) Intereses en común.

   Se observa intereses en común respecto de la información visualizada en el ataque con el perfil analizado: Voto electrónico, Pablo Tonelli, Patricia Bullrich (¿????). Esto significa que por criticar de manera pública y particularmente fundada una cuestión de máximo interés para todos los ciudadanos como lo es todo cuanto se vincula con nuestro proceso electoral, mi defendido tiene un interés común con quien vulnera la seguridad informática de la policía. Un médico ahí.

3) Iniciativa en publicación (concepto de “quema controlada”).

   Se visualizan diversas publicaciones donde Javier Smaldone hace referencia a ataques no se adjudica la autoría, pero da difusión de los mismos generando difusión de los daños generados. A la vez también se visualiza publicaciones en medios periodísticos donde da explicaciones de los mismos como “consultor” o “técnico” (¿????).

   A esto, agrego yo, en los lugares civilizados se lo conoce como periodismo.

4) Análisis temporal causa efecto (modo privado de la cuenta).

   En el marco de la investigación y donde se realizando diversas tareas Javier Smaldone bloquea la visualización a su cuenta actual de twitter (@mis2centavos), si bien se refiere

a un hecho difundido en medios periodístico (https://www.abcdiario.com.ar/espectaculos/2019/8/26/alfredo-casero-explotó-contra-smaldone-que-panquequeada-pegaste-6984.html) a la vez coincide en los momentos de las tareas propias de la investigación (¿????).

Esta afirmación supone que mi defendido estaba al tanto de los contornos de la presente investigación, y justo –justo- cuando la policía intento visualizar su cuenta, el nombrado activó la función de proteger sus twetts. Como si de tal modo pudiese impedir el progreso de la investigación.

5) Hostigamiento hacia el personal policial que investiga causas conexas.

De forma constante y persistente se realizan hostigamientos hacia el personal policial que realizó tareas de investigación manifestando “besis, cabo Landajo” o “Y agarrate, vos, ayudante del cabo Landajo porque te voy a mandar al frente hasta con el color favorito de calzoncillos. Buche de cuarta”. Dicho hostigamiento virtual constante y persistente también, es referenciado en su blog personal (¿????).

A todo evento, pongo en conocimiento del Tribunal que, más allá de enfrentar un hecho inédito en materia social, cuál es la policía quejándose de bulling, mi defendido mantiene una relación pública de tono crítico con dicha fuerza, desde la primera vez que se intentó vincularlo con una investigación criminal. La empezaron ellos.

6) Aversión hacia la policía manifestada en forma pública.

De forma constante se manifiesta aversión hacia la policía (¿????).

7) Publicación de análisis de casos investigados.

Se observa como realiza un análisis detallado de diversos casos obteniendo información de terceras partes (¿????). Nuevamente, en los lugares civilizados a esto se le llama periodismo.

8) Vinculación con actores de causas conexas.

Se observan vinculaciones entre la cuenta analizada y otras cuentas como LIberoamericaMU, Capitan_Alfa, Hispahak (¿????).

Solo diré aquí que en sus más de nueve años de uso de la red social Twitter, con cierto protagonismo en su esfera de conocimiento y habiendo llegado a tener más de treinta y seis mil seguidores, el Sr. Smaldone mantuvo “vinculaciones” con muchísimos usuarios cuya actividad privada ciertamente desconoce.

9) Análisis de información técnico-informático.

En los ataques se visualiza información técnica concordante con las descriptas por el actor tanto en la cuenta de Twitter como así en su CV (¿????).

Se sugiere aquí que por sus conocimientos, mi defendido se encuentra en condiciones de llevar adelante la maniobra investigada. El Sr. Smaldone –y olvidó la policía decir- miles de personas más, solo en nuestro país, que se interesan por la informática.

10) Análisis de información geo-referencial temporal.

Respecto de la información geo-referencial se aprecia lo siguiente: i) misma ubicación entre Emanuel Velez Cheratto y Javier Smaldone son de la Provincia de Córdoba, ii) Javier Smaldone realiza una visita a Santa Fe específicamente en la localidad de Santo Tomé, donde hay vinculaciones con diversas acciones en la referente causa (donde fue como observador electoral colaborando con la Fundación Poder Ciudadano, capitulo argentino de Transparency International). Dicha visita, se omite aclara, ocurrió en el mes de abril de este año, iii) la contratación de Fulltech (Santa Fe 1748) se declara en un domicilio cercano a la ubicación real de Javier Smaldone y iiii) Celulares XIAOMI se generan compras con domicilio de envío en Santa Fe 1635, ubicación cercana a la ubicación real de Javier Smaldone, según información provista por Mercado Libre.

11) Información obtenida mediante pedidos de informes.

Según información analizada de los pedidos de informe a las empresas de telefonía celular, se observan similitudes respecto de los momentos de alta del VPS y solicitud de

baja. Viendo que ambos cuentan con patrones similares de la señal de telefonía celular (¿????). Incomprensible.

Este informe muestra, en mi modo de ver las cosas, que la especie humana, tras siglos de civilización, sigue conservando rasgos bárbaros: en franco desconocimiento del arte de la fundamentación, la línea que separa lo real de lo imaginario aparece aquí un tanto difusa. Basta tener estudios elementales para advertir que mediante este informe se fuerzan, hasta el absurdo, argumentaciones carentes de todo sustento con el único fin de involucrar a mi defendido en el caso. Un método que se utilizaba hace muchos años para canalizar escarmientos.

En ausencia de un mínimo de consistencia intelectual, con estos métodos de investigación, no me sorprende que una investigación naufrague; me sorprende que llegue a puerto.

¿Para esto pagamos tantos impuestos?

Como en muchos informes policiales, lo de menos es lo que dice; lo único que tiene interés es lo que deja afuera: en el caso, el malestar que genera en ciertos ámbitos políticos las investigaciones desarrolladas por el Sr. Smaldone en tanto se vinculan con el voto electrónico.

Vuestras Señorías no tiene porqué saberlo, pero desde hace más de veinte años mi defendido participa públicamente, de manera activa, en distintos debates referidos a cuestiones de máximo interés público. En este último tiempo, ha tenido –dicho modestamente- una participación relevante en todo cuanto se vincula al sistema electoral, más concretamente a la introducción de herramientas informáticas en los procesos de votación y escrutinio, con fuertes críticas a la iniciativa del actual gobierno para la implementación del voto electrónico.

Por estas cuestiones expuso ante el plenario de comisiones de la Honorable Cámara de Diputados y dos veces ante el plenario de comisiones del Senado de la Nación.

Ello, además de haber publicado decenas de notas en diferentes medios de comunicación.

Con base en este informe, con fecha 25 de setiembre pasado, la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina solicitó del instructor distintos procedimientos, entre ellos el allanamiento de un domicilio que mi defendido frecuenta, con el objeto de secuestrar telefonía celular, elementos informáticos, dispositivos de almacenamiento, anotaciones y registros vinculados a la maniobra investigada (fs. 533).

V

Sobre la base de estos antecedentes, con fecha 3 de octubre pasado (fs.591) el instructor dispuso el allanamiento que aquí se cuestiona.

Como ha quedado acabadamente descripto, ni mediando un esfuerzo de imaginación superlativo puede sostenerse que existiese respecto del Sr. Smaldone, a los fines de disponer una orden de allanamiento en el domicilio donde se aloja cuando visita esta Ciudad, motivos, razones o fundamentos que surjan *legítimamente* ni del propio decisorio que aquí se cuestiona, ni de otra pieza procesal a la cual dicho auto remita en forma inequívoca, ni de constancia alguna arrimada al proceso con anterioridad al dictado del mismo, de los cuales surjan de forma indudable la necesidad de proceder.

En modo alguno puede siquiera sugerirse que una medida intrusiva de las características de la que aquí nos ocupa sea una derivación lógica de lo actuado hasta el momento, ni una consecuencia categórica de probanzas colectadas con antelación.

No se puede individualizar en todo el legajo un elemento que autorice lo dispuesto por el Tribunal. Así, la lectura de todo lo actuado no permite tener a la vista las motivaciones de la medida dispuesta, violatoria de disposiciones constitucionales que hacen a la protección del domicilio y de la intimidad de mi defendido.

No puedo pasar por alto que so pretexto de desarrollar una investigación que versa sobre cuestiones tecnológicas, se intentó obtener los datos correspondientes a la tarjeta SUBE y a la

cuenta de *whatsapp* de mi defendido, a la vez que se colocaron cámaras de vigilancia frente a la vivienda de sus hijos, aun en el conocimiento que aquel no se encontraba en el lugar.

Y que estas medidas solo se instrumentaron a su respecto: el resto de las personas involucradas en esta investigación tuvo mejor suerte.

Para disponer un allanamiento, el auto que lo ordena debe sustentarse en una base seria y suficiente para justificarlo. No basta el cúmulo de información **falsa, tergiversada** e **intrascendente** mediante la cual la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina llevó a engaño al Tribunal, formando su convicción acerca de la existencia de motivos legalmente válidos para fundar su proceder.

Por tal motivo, oportunamente se solicitó la declaración de nulidad del auto que ordena el allanamiento cuestionado, y en virtud lo normado en el artículo 172 del Código Procesal Penal de la Nación, la nulidad de todos los actos consecutivos que de él dependen, concretamente, el secuestro verificado en la ocasión.

VI

En la misma dirección, se postuló el dictado de un sobreseimiento respecto de mi defendido, en la inteligencia que no existe el menor indicio (más allá de la imaginación policial) que sugiera que ha participado en la intrusión investigada, o en la difusión de la información así obtenida.

Las maniobras investigadas conllevan el peligro a la seguridad nacional que implica que información propia de las fuerzas de seguridad se encuentre en manos de particulares, que podrían afectar intereses de la República Argentina a partir de la revelación de secretos propios de la Policía Federal Argentina.

Por tal motivo, se dijo, no debía la instrucción permitir que se desvíe el curso de la investigación correspondiente, con la evidente intención de vincular al proceso a personas que

ninguna relación guardan con el mismo, y al amparo de una supuesta investigación dar amparo a seguimientos inadmisibles en el marco de un Estado de Derecho.

VII

Una vez formado el correspondiente incidente, se corrió traslado a las partes de este expediente.

El Señor Fiscal interviniente en autos, Dr. Jorge Felipe Di Lello, sostuvo que nos encontramos en una etapa primaria de la investigación, motivo por el cual, el hecho de adentrarse en el estudio de la cuestión tal como lo pretende esta defensa, no podrá darse sino por las aristas formales de la diligencia en cuestión, so pena de adelantar valoraciones propias de la otra etapa procesal.

Así, el titular de la acción penal dijo que la nulidad formulada intenta valorar los elementos que el instructor tuvo en consideración para el dictado de la medida cuestionada, acudiendo con una lectura diversa sobre la validez de las constancias policiales. Consideró que, a su criterio, la entidad de los informes policiales y de las demás constancias se ven jaqueadas por apreciaciones que, a esta altura, parecen más de una discusión sobre el mérito de la prueba, más que el valor primario y reciente que tienen las definiciones del actuar previsional para fundamentar la diligencia cautelar.

Precisó el Dr. Di Lello que los elementos tenidos en cuenta para el allanamiento fueron resultado del estudio previo de las constancias recolectadas y también de la necesidad expresada por la prevención y ratificada luego por el Tribunal, de contar con elementos que permitieran continuar con la investigación, no surgiendo a su criterio que estuviera presenta la búsqueda de la responsabilidad de Smaldone, pues el nombrado no ha sido el único sindicado por los investigadores, ya que, de hecho, hay otros usuarios, por lo cual no aparece en escena el direccionamiento pesquisitivo hacia él, ni que la decisión judicial responda a otros intereses.

En el mismo sentido, el Representante de la Vindicta Pública estimó que de la lectura del decisorio de fs. 591/606, existe un relato respecto de Javier Smaldone que, prima facie, constituiría una situación que puede sustentar dicha diligencia, y asi conocer las comunicaciones con aquéllos sospechados, como así también otros extremos que son necesarios corroborar y que sólo con las computadoras o su celular pueden determinarse.

Sostuvo también el Señor Fiscal, que entiende y comparte la preocupación que Smaldone transmite con un claro mensaje de preservación de un bien tan preciado por la Constitución Nacional, como es la protección no sólo del debido proceso legal sino de la inviolabilidad de las comunicaciones de los ciudadanos; sin embargo, el ataque a la validez formal de la diligencia en cuestión, no aparece como cuestionable desde donde se intenta, ya que la mera invocación de presentar circunstancias violatorias de derechos, van más allá de dichas garantías, al formar la diligencia aludida una parte de la decisión que involucra a varios usuarios, y que la utilización de distintas comunicaciones y demás constancias probatorias, solo con la información directa puede comenzarse un autentico estudio técnico.

Destacó el Dr. Di Lello que los derechos no terminan allí, sino que el control de la legalidad surge después del secuestro y, a su criterio, ésta no es una prueba que se incorpora al sumario por si, sino que exige una revisión formal y un análisis que extreme los elementos requeridos por el Tribunal, sin sobrepasar tal marco, donde el actuar autorizado no puede resultar atentatorio de sus derechos. Esa es la razón, sostuvo, por la que tomar una decisión sobre la incorporación de la prueba, más en el caso de computadoras o celulares, debe ir acompañada de un examen técnico que satisfaga no sólo a la instrucción sino también a los derechos aludidos y por los que esta parte hoy reclama su reconocimiento, aún a través de una vía que no se comparte como solución procesal.

Por último, consideró que responder a todos y cada uno de los puntos introducidos en la nulidad importaría habilitar la discusión de la prueba en forma temprana, cuando será la instrucción del sumario donde haya tiempo para revisarla, sin dejar de señalar el titular de la

acción penal que los elementos que sirvieron de base para sustentar el registro domiciliario cuestionado, serán materia de análisis a lo largo de la pesquisa y no pueden ser forzados en su entidad probatoria con la sola disconformidad o interpretación del incidentista.

De tal modo, el Señor Fiscal estimó que no puede tener acogida favorable la nulidad introducida.

VIII

Los argumentos vertidos por el Fiscal, receptados por el instructor al resolver el planteo que aqui nos ocupa, son sencillamente inaceptables.

Sin dejar de señalar que algunos párrafos que integran el dictamen del Ministerio Público Fiscal me resultan incomprensibles, por su vaguedad o ausencia de alguna conceptualización en concreto, quiero señalar mi profundo disenso con todo cuanto alli se expone.

Así, esta parte no advierte, ni el señor Fiscal tampoco lo explica, cual es la relevancia a los fines de resolver el planteo que da origen a esta incidencia el hecho de que nos encontremos en una etapa primaria de la investigación.

Tampoco se advierte por qué motivo al resolver un planteo de nulidad se adelantan valoraciones propias de la otra etapa procesal.

Así, el titular de la acción penal señaló que la nulidad formulada intenta valorar los elementos que el instructor tuvo en consideración para el dictado de la medida cuestionada, acudiendo con una lectura diversa sobre la validez de las constancias policiales. Y este es un error de concepto inconcebible, en tanto esta parte señaló y demostró racionalmente que los elementos que se valoraron al dictar la medida cuestionada son falsos, y deben analizarse en el contexto de una persecución judicial impropia de un estado de derecho.

Lo que omite decir en su dictamen el Dr. Di Lello es que los elementos tenidos en cuenta para el allanamiento cuestionado fueron irregularmente concebidos por la policía, y no el

resultado del estudio previo de las constancias recolectadas, y que la necesidad expresada por la prevención y ratificada luego por el Tribunal, de contar con elementos que permitieran continuar con la investigación no hace sino consentir el progreso de una actividad instructoria cimentada sobre una base ilegal, y que no tiene por objeto alcanzar la verdad, ni nada parecido.

No hemos dicho que Smaldone ha sido el único sospechoso sindicado por los investigadores. Hemos dicho que mi defendido ha sido traído a este proceso sobre la base de mentiras que han quedado probadas en el legajo más allá de cualquier duda que pudiese existir.

En el mismo sentido, cuando el Representante de la Vindicta Pública estima que de la lectura del decisorio de fs. 591/606, existe un relato respecto de Javier Smaldone que, prima facie, constituiría una situación que puede sustentar dicha diligencia, omite decir que se trata de un relato falso, construido sobre probanzas tergiversadas de un modo legalmente inaceptable.

Se agradece al Señor Fiscal que entienda y comparta la preocupación que el Sr. Smaldone transmite con un claro mensaje de preservación de un bien tan preciado por la Constitución Nacional, como es la protección no sólo del debido proceso legal sino de la inviolabilidad de las comunicaciones de los ciudadanos; sin embargo, no explica el Dr. Di Lello por qué razón considera que “el ataque a la validez formal de la diligencia en cuestión, no aparece como cuestionable desde donde se intenta, ya que la mera invocación de presentar circunstancias violatorias de derechos, van más allá de dichas garantías, al formar la diligencia aludida una parte de la decisión que involucra a varios usuarios, y que la utilización de distintas comunicaciones y demás constancias probatorias, solo con la información directa puede comenzarse un autentico estudio técnico”.

Por lo demás, al sugerir que tomar una decisión sobre la incorporación de la prueba, más en el caso de computadoras o celulares, debe ir acompañada de un examen técnico que satisfaga no sólo a la instrucción sino también a los derechos aludidos y por los que esta parte hoy reclama su reconocimiento, aún a través de una vía que no se comparte como solución procesal, deja en claro que el Ministerio Público no ha comprendido en absoluto el planteo que nos ocupa.

Pareciera ser, por lo menos asi lo entiendo yo, que el fiscal quiere examinar los elementos secuestrados y luego ver si los incorpora como prueba o no. Y esta parte ha sido muy clara: no existían razones –en lo más mínimo- que autorizacen conforme a derecho los secuestros cuestionados.

Por lo demás, y en términos docentes, es una pena que el Fiscal no diga las razones por las cuales le parece que la vía intentada (un planteo de nulidad) no resulta idónea para canalizar un planteo de nulidad.

Por último, y esto es insólito, el Ministerio Público consideró que responder a todos y cada uno de los puntos introducidos en la nulidad importaría habilitar la discusión de la prueba en forma temprana, cuando será la instrucción del sumario donde haya tiempo para revisarla, sin dejar de señalar que los elementos que sirvieron de base para sustentar el registro domiciliario cuestionado, serán materia de análisis a lo largo de la pesquisa y no pueden ser forzados en su entidad probatoria con la sola disconformidad o interpretación del incidentista.

Una vez más: el momento de revisar la prueba –en tanto se alude a los elementos que sirvieron de fundamento a una orden de allanamiento y secuestro- es ahora. El Código Procesal Penal de la Nación es clarísimo al respecto

Y evidentemente el Dr. Di Lello no ha leído en profundidad nuestro planteo, que no trasluce una disconformidad o diferente interpretación de la entidad probatoria de los elementos que sirvieron de base para sustentar el registro domiciliario cuestionado, sino que ha denunciado una maniobra inaceptable del personal que colaboró con la instrucción que tuvo por objeto vincular de un modo irregular a una persona a un caso del que resulta totalmente ajeno, mintiendo para ello descaradamente.

Al momento de resolver la cuestión, el instructor consideró que el planteo nulificante efectuado esta defensa no puede prosperar, en tanto no se evidencia la violación a la garantía constitucional de defensa en juicio y debido proceso alegada.

Al respecto, señaló que la medida dictada por quien suscribe, -no sólo respecto del incidentista sino respecto de otros catorce domicilios en diversos distritos de la República, tal como surge del auto de fs. 591/606 de los autos principales- se encontró orientada a recabar mayor información en orden a la posibilidad de intensificar la investigación y a los fines de contrastar, efectivamente, las hipótesis desarrolladas por el personal policial –al menos, con las probanzas y análisis glosados a fs. 93/94, 224/231, 240/241, 433/435, 440/441, 515/532, 544 de los autos principales y a fs. 113, 1157/1160, 675/690 del legajo de prueba formado en autos-, con el material electrónico y de comunicaciones que pudiera encontrase en poder de los individuos sospechados, de los cuales llegóse incluso a reclamar el cercenamiento de sus libertades ambulatorias.

Una vez más, se argumenta respecto de cuestiones no planteadas, y se exhiben razones intrascendentes a los fines de resolver el presente planteo.

Es obvio, no existe la menor duda que la medida cuestionada se encontró orientada a recabar mayor información en orden a la posibilidad de intensificar la investigación y a los fines de contrastar, efectivamente, las hipótesis desarrolladas por el personal policial. Lo que esta parte ha planteado es que no existían razones para recabar información en el domicilio del Sr. Smaldone, y que la policía engañó a ese respecto al Tribunal, con elementos falsos.

En consonancia con el parecer expuesto por el Sr. Representante del Ministerio Público Fiscal, el instructor estimó que el cuestionamiento formulado por la defensa no expresa de qué forma le ha sido conculcada la garantía en cuestión, ni tampoco se advierte un perjuicio real y concreto que permita hacer viable el remedio inmediato.

En tal sentido, se invocó un precedente de la Sala II de la Excma. Cámara del Fuero que ha dicho que “Sólo cabe anular las actuaciones cuando el vicio afecte un derecho o interés legítimo y cause un perjuicio irreparable, sin admitirlas cuando no exista una finalidad práctica, que es razón ineludible de su procedencia”. (Cattani- Irurzun- Farah, CCCfed. Sala IIa., causa nro. 27.130 “Boyko, Daniel P. s/ nulidad”, rta. El 23/09/08, reg. Nro. 28.954).

Pareciera ser que el instructor no ha advertido en lo esencial cuanto se desprende de la cita escogida, puesto que si ese fuera el caso, dicho precedente no hace otra cosa que dar razón –de manera contundente- a este defensa.

Así, el instructor ha compartido la línea argumentativa desarrollada por el Ministerio Público –ya rebatida en este escrito-, y en especial rescata una idea elemental e intrascendente, cual es que es justamente la finalidad y meta principal de esta etapa preparatoria construir el objeto del proceso mediante su avance. De tal modo, mediante el desarrollo de esta actividad se irá edificando, progresivamente, el objeto de este legajo, radicando allí la naturaleza de la instrucción. Pues, efectivamente, es durante ella donde se tiende a precisar la imputación, que durante su desenvolvimiento es fluida y puede experimentar modificaciones y precisiones; de allí que durante este procedimiento el objeto resulta construido y es modificable, hasta quedar fijo en la acusación o, en su caso, cuando se la descarta.

Si, claro.

Pero nada de ello puede hacerse violentando garantías constitucionales.

Analizar el informe policial que motiva el allanamiento cuestionado, tanto para el fiscal como para el instructor es algo que no corresponde a esta etapa procesal. Y no puedo más que estar de acuerdo en eso. La diferencia entre mi criterio y el vuestro es que la valoración de estos supuestos indicios que sustentaron la medida que aquí se cuestiona debió haberse hecho antes de autorizar la violación de la intimidad de mi defendido y su pareja y de privarlos de sus herramientas de trabajo y su información personal y profesional.

Luego de exteriorizar una serie de abstracciones cuya relación con este caso no se advierte, no puede dejar de verse que ni el instructor ni el fiscal fueron capaces de señalar un solo elemento que justifique el allanamiento puesto en crisis.

Y sorprende que nadie perciba ninguna violación de derechos, ni tampoco ningún daño.

Se ignora en el caso el respeto por elementales garantías constitucionales, en particular las que refieren a la inviolabilidad del domicilio y de la correspondencia privada, además del

secreto de las fuentes de información periodística (tal el contenido de algunos de los dispositivos que fueron secuestrados).

Más de 35 organizaciones no gubernamentales y grupos de la sociedad civil de 10 países, incluyendo al Consejo Directivo de una Facultad de una Universidad Nacional argentina, se han pronunciado alarmados por la flagrante violación de los derechos del Sr. Smaldone y el peligroso precedente que sientan las medidas adoptadas hasta ahora por la Justicia. El presente caso fue tratado en el Foro de la Gobernanza de Internet realizado en Berlín el pasado mes de noviembre. Entre las organizaciones que se han expresado preocupadas por esta situación, avalando la posición de esta parte, se encuentran algunas tan prestigiosas como Poder Ciudadano y el Centro de Estudios Legales y Sociales —a nivel local— y Amnistía Internacional, Reporteros Sin Fronteras y la Electronic Frontier Foundation —a nivel internacional.

Curioso es, se dijo en su momento, también, que nadie perciba un daño concreto hacia mi defendido. Las fuerzas policiales violaron la intimidad de su domicilio, le quitaron sus herramientas de trabajo y sus datos (dificultando o imposibilitando su actividad laboral, y dañando a sus hijos, ambos estudiantes universitarios a su exclusivo cargo). Y esto además del tiempo insumido por los trámites legales y otras dificultades de índole psicológico (habiendo sido allanado y esposado sin haber hecho absolutamente nada, y viendo que en el expediente no hay ningún elemento real que justifique semejantes medidas, ¿cómo puede estar seguro de conservar su libertad, o de no ser visitado nuevamente por la policía?). El daño concreto, que se intenta evitar con este pedido de nulidad del allanamiento, es la violación de su correspondencia, de información de índole privada, y de información confidencial de naturaleza periodística (amparada en el derecho constitucional de protección de las fuentes).

Recuerdo nuevamente, para finalizar, que en los dispositivos secuestrados se encuentra material confidencial de investigaciones periodísticas finalizadas (que han sido publicadas) y otras que se encuentran en curso, como así también diálogos con varios periodistas argentinos y extranjeros.

IX

En este escenario, luego de realizada la audiencia correspondiente, con fecha 14 de febrero pasado esta Sala resolvió **CONFIRMAR** el auto apelado en todo cuanto decide y ha sido materia de apelación.

Así, en el concepto de V.E. el procedimiento atacado fue ordenado a través de un auto fundado –articulo 123 del del CPPN-, y abarcó numerosos domicilios que se reputaban vinculados con las complejas maniobras informáticas que se busca develar en esta causa. El pronunciamiento glosado a fs. 591/606 remite a los informes policiales agregados previamente, e hizo eco de ciertos indicios preliminares que, en ese momento, postulaban la utilidad de la diligencia en el caso concreto (artículos 193,224 y 225 *in fine* del C.P.P.N.).

Todo ello, vale decir, fue oportunamente avalado tanto por el Juez como por el representante del Ministerio Público Fiscal, se dijo.

Sentado cuanto precede, sin olvidar que la declaración de la nulidad de un acto del proceso es un remedio de naturaleza extrema y de interpretación restrictiva (ver CFP 976/2019/5/CA6 del 06/05/19), la invalidez planteada en la incidencia deviene improcedente. (er CFP 976/2019/5/CA6 del 06/05/19).

En este escenario, no puedo dejar de señalar que:

1. La resolución del Tribunal no se hace cargo, en modo alguno, de los argumentos vertidos por la defensa en la ocasión procesal pertinente. Cierto es que el Tribunal no esta obligado a dar respuesta a la totalidad de las cuestiones planteadas por la defensa, pero

en el caso no ha dado respuesta a ninguna, ignorando de este modo atender el planteo efectuado.

2. Sostiene V.E. que el procedimiento atacado fue ordenado a través de un auto fundado –articulo 123 del del CPPN-, y abarcó numerosos domicilios que se reputaban vinculados con las complejas maniobras informáticas que se busca develar en esta causa. El pronunciamiento glosado a fs. 591/606 remite a los informes policiales agregados previamente, e hizo eco de ciertos indicios preliminares que, en ese momento, postulaban la utilidad de la diligencia en el caso concreto (artículos 193,224 y 225 *in fine* del C.P.P.N.).

3. Debe tenerse en cuenta, al respecto, que más allá de lo que se haga constar en el auto que dispone el allanamiento, lo que resulta **esencial** para que un allanamiento se ajuste a las pautas constitucionales es que del expediente surjan los motivos que le dieron sustento. Por ello, el juez o tribunal que deba analizar un caso en el que se cuestione la validez de un allanamiento deberá siempre estudiar los extremos objetivos agregados al expediente, sea que en el auto de allanamiento y en la orden se hayan hecho constar los motivos de acto o no.

4. Va de suyo que un auto de allanamiento en el que se hicieren constar los motivos del mismo puede llegar a facilitar la tarea apuntada, pero esto, sin embargo, es relativo, ya que puede dares el caso de un auto de allanamiento en el que se consignara con sumo detalle una serie de motivos para fundarlo que, en realidad, no existan, o al menos, no consten en el expediente. En tal supuesto, tendríamos un “auto fundado” pero en modo alguno tendríamos un allanamiento llevado a cabo conforme a la Constitución, pues en tal caso (nuestro caso) el ineludible estudio de las constancias del expediente nos llevaría a concluir que, en realidad, se trató de un allanamiento constitucionalmente inválido por no estar sustentado en elemento previo, objetivo y razonable alguno.

5. Y esta parte ha sostenido y demostrado, de manera contundente, a) que el auto fundado reseña elementos de análisis objetivamente falsos (perfectamente individualizados), maliciosamente incorporados al legajo por la fuerza policial, b) que los informes policiales agregados previamente no incluyen ningún dato relevante que pueda justificar una medida intrusiva de las características de la que aquí se cuestiona, c) que los indicios preliminares invocados no solo no superan el mínimo margen de seriedad, sino que proyectan una preocupante prerrogativa a la fuerza policial, quien argumentando de un modo desopilante puede de este modo, vincular a cualquier ciudadano con cualquier investigación en curso y d) que no existe en el caso elemento objetivo idóneo alguno para fundar una mínimo sospecha razonable que autorizase el allanamiento que aquí se cuestiona (La mera expresión de sospecha de un funcionario judicial no constituye, per se, esa base objetiva).

6. Así, no hemos sostenido, como parece entender V.E., que la medida no tiene fundamento. Hemos dicho que la medida tiene un fundamento esencialmente ilegal, construido adrede por la Policía Federal Argentina, orientado a vincular a mi defendido con un hecho con el cual no tiene la menor vinculación.

7. Como ha quedado acabadamente descripto, ni mediando un esfuerzo de imaginación superlativo puede sostenerse que existiese respecto del Sr. Smaldone, a los fines de disponer una orden de allanamiento en el domicilio donde se aloja cuando visita esta Ciudad, motivos, razones o fundamentos que surjan *legítimamente* ni del propio decisorio que aquí se cuestiona, ni de otra pieza procesal a la cual dicho auto remita en forma inequívoca, ni de constancia alguna arrimada al proceso con anterioridad al dictado del mismo, de los cuales surjan de forma indudable la necesidad de proceder.

8. En modo alguno puede siquiera sugerirse que una medida intrusiva de las características de la que aquí nos ocupa sea una derivación lógica de lo actuado hasta el momento, ni una consecuencia categórica de probanzas colectadas con antelación.

9. Así, no se puede individualizar en todo el legajo un elemento que autorice lo dispuesto por el instructor. La lectura de todo lo actuado no permite tener a la vista las motivaciones de la medida dispuesta, violatoria de disposiciones constitucionales que hacen a la protección del domicilio y de la intimidad de mi defendido.

10. V.E., se dijo, omitiendo tratar el planteo introducido por esta defensa, ha señalado de manera genérica las razones que permiten sostener la medida cuestionada. Pero esta a la vista que no ha dado acabado tratamiento a los planteos de mi parte, en tanto no ha dado respuesta a ninguno de los cuestionamientos oportunamente introducidos.

11. Enfrentamos así una respuesta dogmática, alejada por completo del menor análisis de las constancias agregadas al legajo. Este defecto de fundamentación constituye una causal definida de arbitrariedad por la CSJN, ya que resiente la motivación lógica del fallo y desatiende el mandato del artículo 123 del Código Procesal Penal de la Nación que reglamenta la garantía constitucional de la defensa en juicio y el debido proceso (artículo 18 Constitución Nacional), en cuanto exige que las decisiones judiciales sean fundadas y constituyan una derivación razonada del derecho vigente en relación con las circunstancias comprobadas de la causa.

12. Es claro para esta parte que, una vez compulsados por el instructor, sin ningún motivo válido que lo autorice, los elementos secuestrados en autos pertenecientes a mi defendido, sus pretensiones de defender su intimidad quedaran pulverizadas –imposible repararlas ulteriormente-. Y lo que es peor, quedará legitimada la posibilidad (de una gravedad inusitada) de que la policía, o cualquier fuerza de seguridad, vincule a un ciudadano inocente con un hecho criminal sobre la base de mentiras.

13. *La omisión del juez de decidir una cuestión propuesta oportunamente y conducente a la solución del pleito ha sido tratada por nuestra Corte Suprema de Justicia de la Nación en los siguientes casos: 1) "Verdun, Vicente c/ENCOTEL", del 15 de octubre de 1996 (la Ley, 1997-B, 196), donde se dijo que "...el punto central de la controversia consistía en*

determinar la virtualidad de las modificaciones introducidas en el Convenio Colectivo de Trabajo 32/75 mediante ley 21.476 y el dec. 3591/77... resultando indispensable el tratamiento de la tacha de inconstitucionalidad de dichas normas que el actor articuló en su demanda y mantuvo en las sucesivas etapas del proceso". No habiéndolo hecho así, al no pronunciarse sobre el punto constitucional propuesto, la sentencia era descalificable con base en la doctrina de la arbitrariedad, produciéndose "un grave menoscabo al derecho de defensa en juicio"; 2) "Aadi Capif Asociación Civil Recaudadora c/Establecimiento Kronas y otro", del 12 de agosto de 1997 (La Ley, 1998-A, 105), la sentencia fue descalificada por haber omitido "el tratamiento de argumentos oportunamente propuestos y conducentes para la correcta solución del caso"; 3) "Troche Báez, Postracio c/Olivadese e Hijos S.R.L., Salvador", del 26 de agosto de 1997 (La Ley, 1998-B, 776), donde se dijo que "... el tribunal omitió considerar constancias incorporadas a la causa y prescindió del examen de planteos oportunamente introducidos y conducentes para la solución de la litis"... por lo que"...en tales condiciones, el fallo no satisface el requisito de constituir una derivación razonada del derecho vigente con la aplicación a las circunstancias del caso, por lo que ante la relación directa existente entre lo resulto y las garantías constitucionales de igualdad y defensa en juicio, corresponde descalificar la sentencia con fundamento en la doctrina de esta Corte sobre arbitrariedad"; 4) "Neustadt, Bernardo" del 17 de marzo de 1998 (La Ley, 1998-C, 786) en este caso cinco jueces declararon la inadmisibilidad del recurso extraordinario con cita del art. 280 del Código Procesal Civil y Comercial; el voto disidente de los jueces Moliné O' Connor, Fayt y Boggiano, así como también el voto disidente de Petracchi, señalaron que el tribunal apelado "...omitió pronunciarse sobre una cuestión esencial para la solución del caso, oportunamente planteada por la querella, cual es la referente a la existencia de diversos actos procesales que -según el criterio del acusador- constituirán secuela de juicio, con entidad suficiente para

interrumpir la prescripción"...y "que la omisión a que se ha hecho referencia descalifica la decisión recurrida con sujeción a la doctrina sobre arbitrariedad, ya que afecta en forma directa e inmediata la garantía de la defensa en juicio"; 5) "Ungaro, Albor c/Martinez, Enrique L. y otra", del 17 de marzo de 1998 (La Ley, 1998-C,788), por el voto de cinco jueces se decidió que "...el pronunciamiento omitió tratar un tema que resultaba esencial para la adecuada solución de la litis. Ello es así, pues la índole del planteo exigía dilucidar si la decisión de la justicia ordinaria provincial importaba la injustificada privación de una base regulatoria mediante la fijación de pautas irrazonables, que no resultaban susceptibles de revisión por el juez al que se encomendó determinar los estipendios.... Lo expuesto conduce a la descalificación del fallo como acto jurisdiccional válido en los términos de conocida doctrina de esta Corte en materia de arbitrariedad y hace innecesario el tratamiento de las demás cuestiones de índole constitucional propuestas por el apelante". Tres jueces decidieron que el recurso extraordinario era inadmisible, con referencia al art. 280; 6) "De Gregorio de Scalas, Santa c/Caja Nac. de Prev. para Trabajadores Autónomos", del 7 de mayo de 1998 (La Ley, 1998-D,693) donde la mayoría (6 jueces) establecieron que "el a quo, con menoscabo del derecho de defensa en juicio, omitió tratar planteos oportunamente deducidos y conducentes para la correcta resolución de la causa, valorar pruebas regularmente incorporadas, y condujo a la pérdida de derechos que cuenten con amparo constitucional (arts. 14 bis y 18, Constitución Nacional)... Que resulta oportuno señalar que esta Corte ha decidido que es arbitraria la sentencia que se limita a un análisis aislado de los diversos elementos de juicio obrantes en la causa pero no los integra ni los armoniza debidamente en su conjunto, lo cual lleva a desvirtuar la eficacia que, según las reglas de la sana crítica, corresponde a los distintos medios probatorios (Fallos:308:112, 640; 311:948 -La Ley 1987-A, 114; 1988-E, 395-), vicio que impone descalificar al pronunciamiento es este aspecto (Fallos: 303:2080)".

14. Surge con claridad de la jurisprudencia mayoritaria que la omisión de un tribunal de tratar una cuestión esencial llevada al debate descalifica cualquier fallo como acto jurisdiccional válido en los término de la conocida doctrina de nuestra Corte Suprema de Justicia de la Nación en materia de arbitrariedad. Sobre esta base fundamos este recurso.

15. Sobre la base de lo expuesto, esto es, que V.E. no ha dado respuesta satisfactoria a una cuestión propuesta por la defensa que resultaba conducente para variar la solución del pleito, resulta menester que se examinen cuáles son los presupuestos que condicionan la emisión de una orden de allanamiento de modo compatible con la garantía de la inviolabilidad del domicilio.

16. En esa dirección, nuestra Corte Suprema de Justicia de la Nación ha señalado en numerosas oportunidades la obligación que incumbe a los jueces de fundar sus decisiones, y esto es, no solamente porque los ciudadanos puedan sentirse mejor juzgados, ni porque se contribuya así al mantenimiento del prestigio de la magistratura. La exigencia de fundamentación de las decisiones judiciales persigue también la exclusión de decisiones irregulares, es decir, tiende a documentar que el fallo de la causa es derivación razonada del derecho vigente y no producto de la voluntad individual del juez. La decisión del juez que ordena un allanamiento debe ser fundada, pues la motivación de la decisión es el modo de garantizar que el registro aparece como fundadamente necesario. El control judicial esta impuesto en el caso por la necesidad de controlar la coacción estatal y evitar la arbitrariedad de sus órganos: si los jueces no estuvieran obligados a examinar las razones y antecedentes que motivan el pedido de las autoridades administrativas y estuviesen facultados a expedir ordenes de allanamiento sin necesidad de expresar fundamento alguno, la intervención judicial carecería de sentido, pues no constituiría control ni garantía alguna para asegurar la inviolabilidad del domicilio.

17. Sobre la base de lo expuesto, insisto, los defectos de procedimiento señalados importan una afectación a la garantía de inviolabilidad del domicilio. La Constitución Nacional en su artículo 18, determina como regla general que el domicilio es inviolable, estableciendo, a su vez, que excepcionalmente se podrá proceder a su allanamiento y ocupación cuando concurran los casos y justificativos que una ley previa deberá consignar. Este mandato de protección legal contra las injerencias abusivas o arbitrarias del Estado en el domicilio de los ciudadanos también está contenido en los pactos internacionales investidos de rango constitucional en virtud del artículo 75 inciso 22 de nuestra ley suprema; en particular, artículos 9 de la Declaración Americana de los Derechos y Deberes del Hombre; 12 de la Declaración Universal de Derechos Humanos, 11.2 de la Convención Americana sobre Derechos Humanos y 17 del Pacto Internacional de Derechos Civiles y Políticos.

18. Por lo demás, aun cuando las críticas que aquí se formulan conducen al examen de cuestiones de hecho, prueba y derecho procesal, en la medida que esos aspectos se encuentran relacionados directamente con el alcance que cabe atribuir a la garantía de la inviolabilidad del domicilio, esta parte entiende que ellas constituyen cuestión federal suficiente.

X

En virtud de lo dicho, ante la eventualidad de una solución adversa a la que se propone, mantengo la reserva del caso federal en razón de los agravios constitucionales señalados en este escrito.

XI

En virtud de todo lo expuesto, habré de solicitar de V.E. que conceda el presente recurso de casación, interpuesto en legal tiempo y forma, y eleve todo lo actuado a conocimiento del Superior, a los fines que resuelva en definitiva

Tener presente lo expuesto,

SERÁ JUSTICIA

PRESENTA ESCRITO COMO “AMIGO DEL TRIBUNAL”

Cámara Federal de Casación Penal,

Comodoro Py 2002

La **Fundación para la Difusión del Conocimiento y el Desarrollo Sustentable “Vía Libre” (en adelante Fundación Vía Libre)**, representada en esta ocasión por su presidente **María Beatriz Busaniche**, con el patrocinio letrado de Martín Pablo Silva Valent, T120 F2 CPACF, constituyendo domicilio procesal en la calle [redacted] de la Ciudad Autónoma de Buenos Aires, con correo electrónico info@vialibre.org.ar y domicilio electrónico en [redacted], en el marco de la Causa **Nro. 55276/2019 radicada en el Juzgado Nacional en lo Criminal y Correccional Federal Nro. 9, Secretaría Nro. 18, “Smaldone, Javier s/ incidente de nulidad”** en conocimiento de esta **Sala 3 de la Cámara Federal de Casación Penal**, nos presentamos y respetuosamente decimos:

I. PERSONERÍA

María Beatriz Busaniche es Presidente de la Fundación Vía Libre según constancia de actas Nro. 223 con fecha 24 de Agosto de 2018 y en tal carácter se encuentra expresamente autorizada a representar a la organización en la presente acción de conformidad con el art. 15 del Estatuto de la organización. Se adjunta copia fiel del original del Estatuto de la Fundación Vía Libre.

La Fundación Vía Libre es una organización civil sin fines de lucro radicada en la Provincia de Córdoba con registro ante la Inspección de Personas Jurídicas fechado el 28 de noviembre de 2000 y tiene como objeto estatutario “*promover la libertad y la cooperación para la difusión del conocimiento en general; promover la libertad de las personas, grupos,*

asociaciones, comunidades, fundaciones, empresas de acceder, difundir, estudiar, desarrollar, mejorar el conocimiento en general y de esta manera promover el mejoramiento económico y social de los grupos antes mencionados; promover la capacitación, el crecimiento, la organización y el desarrollo sostenible de grupos, asociaciones, fundaciones, empresas, sean estas urbanas o rurales permitiendo el acceso de estas a los beneficios de la sociedad global; fomentar y difundir las actividades de estudio e investigación y desarrollo en todas las ramas de las ciencias, la cultura y las artes en general; atendiendo en todo ello, de manera especial a los sectores menos desarrollados, utilizando para cumplir los objetivos antes mencionados la difusión, promoción y creación de software libre sin que esto constituya limitante alguno para utilizar otras herramientas lícitas y legales en pos de lograr los objetivos mencionados en este artículo."

En este sentido, la Fundación Vía Libre trabaja desde hace 20 años en directa relación con la comunidad informática de la Argentina en la difusión, promoción y acceso al conocimiento de las múltiples ramas de la informática esenciales para el desarrollo sustentable y la incorporación de tecnologías a la vida pública desde una perspectiva respetuosa de los derechos humanos fundamentales en el marco de las garantías vigentes en la Constitución Nacional.

La Fundación articula sus acciones de manera permanente con organizaciones afines a nivel nacional e internacional, trabaja en incidencia pública sobre políticas de estado de utilización de tecnologías apropiadas, en particular de Software Libre, a fin de cumplir con las metas de desarrollo social y económico del milenio. En este sentido, la Fundación Vía Libre actúa en diferentes temáticas entre las que se incluyen: seguimiento de políticas de propiedad intelectual y acceso al conocimiento, políticas de privacidad y protección de datos personales, incluyendo dentro de ellas, la promoción de sistemas que garanticen el debido proceso, el acceso a la justicia, la inviolabilidad de las comunicaciones y el domicilio y la protección de la vida privada en toda su amplitud, tanto en el espacio privado como en la esfera pública, políticas de incorporación de tecnologías en procesos electorales desde la perspectiva de derechos civiles y políticos, regulaciones de Internet

y políticas de seguridad en el entorno digital y la protección legal de la comunidad de seguridad informática a fin de que pueda desarrollar plenamente sus tareas de prevención, investigación, análisis y reporte de vulnerabilidades en los sistemas informáticos.

II. OBJETO

La Fundación Vía Libre viene a presentarse como Amigo del Tribunal (Amicus Curiae) a los fines de acercar a este Tribunal consideraciones relativas a la cuestiones de derechos fundamentales y derechos humanos del Sr. Javier Smaldone involucradas en la causa de referencia, cuyo precedente tendría un impacto masivo en los derechos humanos y fundamentales y su ejercicio en toda la Nación.

Sobre la base de los fundamentos que a continuación se exponen, solicita se tenga a la Fundación Vía Libre y a los propios peticionantes por presentados en el carácter invocado, se incorpore este documento al expediente de referencia, sin perjuicio de ampliar oralmente los argumentos si así lo resolviera ese Tribunal, y se lo tenga en cuenta al momento de resolver.

III. ADMISIBILIDAD

1. Que conforme el precedente “CORONADO AYLLON, Alicia s/recurso de casación”, sentencia de 15 de febrero de 2018 de la CAMARA FEDERAL DE CASACION PENAL SALA 4, FSA 13438/2016/TO1/4/1/CFC1, que sostiene *“I- En primer lugar, cabe apuntar que la actuación de los amigos del Tribunal encuentra apoyatura en el sistema interamericano –art. 63.2 del Reglamento de la Corte Interamericana de Derechos Humanos, habiendo sido autorizado por la Comisión Interamericana de Derechos Humanos con sustento en los arts. 44 y 48 de la C.A.D.H., el cual encuentra jerarquía constitucional en nuestro sistema normativo (art. 75, inciso 22 de la C.N.).*

Además, nuestro máximo tribunal ha reconocido y reglamentado la actuación de los amicus curiae ante la Corte Suprema de Justicia de la Nación, mediante la Acordada No 7/13. "; y conforme a CFP 1302/2012/TO1/26/CFC9; queda sin lugar a dudas la existencia, legitimidad y oportunidad de la institución de Amicus Curiae. Toda vez que el presente Amicus Curiae que se pretende está dentro de los plazos, justificado su interés, relevancia jurídica de la situación a decidir y aporta argumentos jurídicos relevantes a esa decisión. Siendo que la cuestión tratada en estos autos es de interés público dado que su solución podría derivar en la afectación directa de la presunción de inocencia, la libertad de expresión, el principio de legitimidad, privacidad y todos los derechos tutelados que en conexión necesaria con estos se ven afectados ante la arbitraria y errónea interpretación de los hechos, la determinación y prueba de los hechos en sí mismos, y derechos alegados en la causa.

La Fundación Vía Libre manifiesta su interés de concurrir a esta causa como amigo del tribunal con base en las siguientes consideraciones:

La Fundación Vía Libre trabaja desde hace 20 años en asistir a tomadores de decisiones de políticas públicas en aspectos vinculados a las regulaciones de Internet. La misión de la organización es promover debates tendientes a establecer los principios de Derechos Humanos como rectores en el diseño de políticas y regulaciones en los diversos campos de trabajo de la Fundación. Desde esta perspectiva, el trabajo permanente con legisladores nacionales, funcionarios del poder ejecutivo, la participación en foros de políticas regionales y globales, y el seguimiento de los debates asociados a las tecnologías digitales y los derechos humanos son parte ineludible de la actividad de la Fundación, que también promueve el debate ciudadano en la materia.

La organización es, en su campo, una de las instituciones más reconocidas a nivel nacional y regional en la materia y es consultada regularmente por funcionarios públicos, legisladores de diferente origen partidario, activistas y organismos de la sociedad civil así como por contrapartes de toda la región.

Desde sus inicios, la Fundación Vía Libre trabaja con la comunidad de seguridad informática local en diversos temas de interés público entre los que se destacan tres que tienen vínculo directo con el expediente de referencia: a) las políticas de seguridad pública y la protección de las garantías constitucionales en la investigación criminal, el seguimiento de servicios de inteligencia así como la adopción de tecnologías de vigilancia en materia de seguridad y privacidad, b) las políticas de adopción de tecnologías en procesos electorales incluyendo las experiencias de voto electrónico en la Argentina y en la región, c) Las preocupaciones legales de la comunidad de seguridad de la información frente a la legislación vigente en materia de delitos informáticos y a la práctica habitual de investigación penal en la materia.

En este sentido, Vía Libre tiene una larga trayectoria de trabajo con la comunidad técnica con la que ha desarrollado cooperación y actividades conjuntas a fin de promover la adopción responsable de tecnologías en la vida social, prevenir los impactos negativos que estas pudieran tener sobre la vida ciudadana y garantizar el pleno respeto de los derechos humanos y el marco de garantías constitucionales en la implementación de tecnologías, en la investigación y en el trabajo de seguridad informática.

2. La Fundación sostiene que la inviolabilidad del domicilio, la privacidad y el debido proceso judicial están en riesgo si no se reconoce y declara la nulidad del allanamiento del domicilio del Sr. Javier Smaldone y se devuelven los equipamientos informáticos retenidos por la fuerza pública en el mencionado acto procesal ordenado por el Juez Rodríguez en primera instancia.

3. Ni Fundación Vía Libre ni sus miembros del Consejo de Administración que se presentan aquí por propio derecho han recibido ni recibirán de ninguna de las partes resarcimiento ni compensación de ningún tipo que se relacione con esta presentación. Tampoco obtendrán beneficio patrimonial alguno, directo o indirecto, como resultado de proceso. El Sr. Javier Smaldone, a quien acompañamos en esta presentación como amigos del tribunal no forma parte de la Fundación Vía Libre pese a que ha

contribuido de manera *ad honorem* y en forma regular como colaborador voluntario en algunas de las acciones realizadas por nuestra Fundación en la campaña por la concientización sobre los riesgos del voto electrónico en la Argentina y la región.

4. Nuestro interés en el caso se basa en la falta absoluta de argumentos que sostengan la orden de allanamiento y posterior requisa de elementos informáticos del Sr. Smaldone, por lo que no declarar la nulidad de lo actuado no sólo avasalla los derechos fundamentales de la persona involucrada, sino que deja sentado un precedente de gravedad jurídica indudable.

IV. ARGUMENTOS

El allanamiento cuya nulidad se reclama en este acto, “N.N y otros s/ violación de correspondencia, intimidación pública y violación de sistemas informáticos”, contempla la investigación de las filtraciones de información de la Policía Federal Argentina y carece de imputados al día de la fecha. En ese marco, el Sr. Javier Smaldone, a través de sus diversos medios sociales de comunicación, hizo público el hecho, y al igual que muchos otros expertos en el tema y periodistas advirtió sobre la gravedad de las filtraciones de información de los sistemas de correo electrónico de las fuerzas de seguridad federales e indicó públicamente la seriedad de tal suceso, especialmente considerando la necesidad de preservar la integridad de las personas involucradas en las comunicaciones filtradas.

El Sr. Smaldone tiene conocimientos de informática y una de sus áreas de trabajo es la seguridad informática y la difusión de buenas prácticas en relación al cuidado y protección de la información, en particular, la información de carácter sensible cuya divulgación puede implicar riesgos para las personas involucradas, y ya en muchas otras ocasiones se ha ocupado de informar públicamente sobre filtraciones similares que afectaron tanto información de las fuerzas de seguridad como de la ciudadanía en general.

Una revisión detallada del expediente indica que las únicas justificaciones presentadas para el allanamiento sobre el cual se realiza el planteo de nulidad, tienen que ver con las manifestaciones públicas del Sr. Smaldone sobre este y otros casos similares, así como sus conocimientos de informática. Si se avala un procedimiento de este tipo no sólo habrá una colisión clara con los principios fundamentales de libertad de expresión, sino que se dejará asentado que los meros conocimientos de un área fundamental como la informática y la seguridad de los sistemas de información pueden convertir a una persona inocente en sospechoso sin más.

Es por eso que consideramos el caso de interés público. Por esa razón nos presentamos ante este tribunal y por esa misma razón presentamos, junto a otras organizaciones de la sociedad civil, un escrito ante el Juzgado competente.

Los indicios presentados por la policía llaman la atención por su arbitrariedad y fragilidad. En primer lugar, convierten en presunto sospechoso a Smaldone por el mero hecho de tener conocimientos especializados en seguridad informática y, en segundo lugar, sospechan de su participación en este acto por las publicaciones que realizó en redes sociales y sus opiniones respecto del caso (véase “indicios” página 515 del expediente). El juez de la causa consideró suficientes estos indicios para autorizar el acceso a información sensible de Smaldone, incluyendo el requerimiento de su geolocalización a proveedores de telefonía móvil, el pedido de información a su proveedor de Internet, la intervención de sus comunicaciones privadas, la instalación de cámaras de vigilancia en los alrededores de su domicilio, la solicitud de seguimiento de sus movimientos a partir de informes sobre el uso de su tarjeta de transporte público, el allanamiento de su domicilio, el secuestro de sus dispositivos personales y herramientas de trabajo y su demora por 6 horas en una dependencia policial para la presunta investigación de antecedentes de los que carece.

De los indicios señalados, sin embargo, no se desprende ningún hecho o circunstancia sólidas que revistan carácter suficiente para constituir

una sospecha fundada que autorice las graves medidas emprendidas. La Corte Suprema de Justicia Argentina ya afirmó que la intervención y el acceso a datos relativos a la comunicación deben cumplir con un análisis suficiente de necesidad y proporcionalidad de la restricción del derecho del investigado. Asimismo el Código Procesal Penal Federal establece la razonabilidad como parte del examen que debe hacer el juez cuando autorice medidas de comprobación directas como el allanamiento (art. 144).

Tanto el estándar legal para acceder a los datos, como la necesidad y proporcionalidad de las medidas, son requisitos establecidos en estándares internacionales de derechos humanos. Así lo explican los “Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones”, producto de una consulta global con grupos de la sociedad civil, la industria y expertos en la materia. Esos principios establecen que toda medida que implique una privación de un derecho fundamental sólo puede estar justificada cuando es prescrita por la ley, es necesaria para lograr un objetivo legítimo, y es proporcional al objetivo perseguido.

Es más, la argumentación de la Cámara Federal de Apelaciones para rechazar el pedido de nulidad del allanamiento carece de fundamentos y remite a actuaciones preexistentes sin ninguna relación con la causa de referencia.

El trabajo de los investigadores en seguridad informática está protegido por el derecho a la libertad de expresión. Esto surge de la interpretación amplia de la jurisprudencia y la doctrina del artículo 13 de la Convención Americana de Derechos Humanos. Es un comportamiento usual para los investigadores monitorear, comentar y criticar información relacionadas a su expertise técnico en las redes sociales o en medios periodísticos. Por eso, en el caso de Javier Smaldone, su opinión técnica y crítica no debería ser vista como sospechosa, sino como una demostración de sus conocimientos técnicos y su voluntad de cooperación a favor de la seguridad de los sistemas informáticos. Más aún, y específicamente en relación al caso de Smaldone, la libertad de expresión abarca el derecho a

impartir información, es decir, a publicar y alertar sobre la existencia de vulnerabilidades en sistemas informáticos, con el objetivo de concientizar para su solución. Existe también aquí un interés social en conocer sobre fallas en sistemas esenciales para el ejercicio y la protección de los derechos de los ciudadanos. Es particularmente sensible e indispensable entender lo que ha ocurrido en un caso en el cual se está investigando a quienes reportaron públicamente lo sucedido, y no a los reales responsables de la filtración, que parece más basada en un acto de negligencia que en un ataque sofisticado contra los sistemas de la Policía Federal.

Sería más apropiado que la Justicia investigue lo actuado por las fuerzas de seguridad en todo el proceso de investigación criminal a fin de garantizar la protección de los derechos fundamentales. Entre otras cosas, es rol de la Justicia sopesar la calidad de los pedidos de investigación y rechazar los avances sobre la vida privada de las personas, en este caso, del Sr. Smaldone y su familia, sin sospechas debidamente fundadas y evitar la utilización del sistema penal como respuesta al trabajo de los investigadores en seguridad informática.

En el mismo sentido que nosotros se han pronunciado públicamente y ante el juez competente organizaciones de derechos humanos a nivel nacional tales como el Centro de Estudios Legales y Sociales (CELS) y Poder Ciudadano, entre otras de carácter internacional como Freedom House, Electronic Frontier Foundation y AccessNow.

Vale mencionar, a modo de ejemplo, que la organización internacional de libertad de expresión y Derechos Humanos Freedom House, en su reporte del año 2020 mencionó especialmente la situación de persecución de expertos en seguridad informática como elemento crítico en Argentina, mencionando como ejemplo el caso del Sr. Smaldone.

Por lo antedicho, solicitamos se nos tenga por presentados ante este tribunal en calidad de amicus curiae, solicitamos la declaración de nulidad del allanamiento sobre el domicilio del Sr. Smaldone y la inmediata devolución de sus dispositivos y otros bienes y elementos de trabajo

retenidos durante el procedimiento sobre el cual se invoca nulidad sin que se avance bajo ninguna circunstancia sobre la privacidad de los mismos.

V. CONCLUSIONES

Nuestro propósito en esta presentación ha sido dejar constancia de que:

- Los principios de inviolabilidad del domicilio están en riesgo si se avanza en legitimar un allanamiento carente de todo fundamento por el mero hecho de que la persona involucrada se ha pronunciado abiertamente en redes sociales en relación a un caso de interés público y por sus conocimientos de informática.
- Los principios de libertad de expresión del Sr. Smaldone en particular, y de la comunidad de seguridad informática en general, se ven avasallados si por el tenor de sus conocimientos se ven amenazados de emitir opiniones y difundir información de interés público vinculada a su área de expertise.
- El debido proceso y las garantías judiciales deben prevalecer en este caso donde a todas luces el allanamiento sobre el cual de invoca nulidad carece de fundamentos y vinculaciones probadas con la causa de marras.
- Finalmente, el allanamiento, demora y averiguación de antecedentes de una persona por el sencillo hecho de informar al público sobre un caso de gravedad institucional severa dentro de las fuerzas de seguridad federales debería llamarnos a la reflexión sobre la calidad de la investigación en marcha y el riesgo que las propias fuerzas de seguridad corren si sus sistemas de información son tan fácilmente vulnerados y filtrados.

VI. PETITORIO

Por lo expuesto, a V.E. se solicita:

1. Se declare la admisibilidad del presente escrito como “Amigo del Tribunal”.
2. Se tenga por presentada la copia del estatuto de la Fundación Vía Libre.
3. Se incorpore el presente escrito al expediente y se corra traslado a las partes en caso de que V.E. lo considere pertinente.
4. Oportunamente, al momento de resolver se tengan en cuenta los argumentos jurídicos y técnicos expuestos en esta presentación.

Provéase de conformidad que,

SERÁ JUSTICIA

María Beatriz Busaniche

Presidente

Fundación Via Libre

Martín Pablo Silva Valent

Abogado

T120 F2 CPACF

MANIFIESTA – SOLICITA

–Por lo demás este caso no puede ser muy relevante,
lo infiero del hecho de ser acusado sin que pueda
determinar la falta que justifique tal acusación.
Pero estimo que también esto es secundario.
Lo esencial es saber concretamente de qué soy acusado
y qué autoridad dirige el procedimiento pertinente.

(Franz Kafka, "El Proceso")

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], conjuntamente con mi abogado defensor Pablo Slonimsqui, en autos caratulados "N.N.Y OTROS S/VIOLACIÓN DE CORRESPONDENCIA, INTIMIDACIÓNPUBLICA Y VIOLACIÓN SIST. INFORMÁTICO ART.153 BIS1°PÁRRAFO DENUNCIANTE: LA ROCCA, MARIO Y OTROS" Expte N.º 55276/2019 que tramitan en la Secretaría n° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V. S. respetuosamente digo:

I

Que el día 8 de octubre de 2019 vi violada la privacidad de mi domicilio (***artículo 12*** *de la Declaración Universal de Derechos Humanos y* ***artículo 18*** *de la Constitución de la Nación Argentina*) a raíz de una afirmación falaz del subcomisario Carlos Alberto Aguirre, quien en la declaración que consta a fs. 68 me hizo responsable de un hecho que aún no fue juzgado —y en cuya investigación nunca estuve siquiera imputado— complementada con un ridículo informe policial —que ya he desacreditado punto por punto a fs. 1157-1180 y a la fecha he utilizado como ejemplo de *mala praxis* en varias conferencias de especialistas en tecnología y seguridad informática— basado en gran parte en mis opiniones políticas vertidas públicamente en la red social Twitter (***artículo 19*** *de la Declaración Universal de Derechos Humanos,* ***artículo 19*** *del Pacto Internacional de Derechos Civiles y Políticos*). En dicha oportunidad también se me privó de mi libertad (fs. 738) —a mi juicio, ilegítimamente— durante 12 horas: las 6 que duró el operativo en mi domicilio y otras 6 en dependencias policiales (***artículo 3*** *de la Declaración Universal de Derechos Humanos)*.

Que desde ese entonces se me ha privado de mi propiedad y de mis datos (***artículo 17*** *de la Declaración Universal de Derechos Humanos)* al mantener secuestrados elementos de trabajo que contienen información sin la cual me ha sido imposible realizar mis tareas, lo que me ha

generado pérdidas económicas (***artículo 23*** *de la Declaración Universal de Derechos Humanos)*.

Que también desde hace más de 16 meses se ha conculcado mi derecho a la honra (*nuevamente,* ***artículo 12*** *de la Declaración Universal de Derechos Humanos)*, ya que las mismas fuerzas policiales que me incriminaron falsamente en la causa de marras, también se dedicaron a ventilar a los medios acusaciones que no se animaron a volcar en el expediente. Así es como aparezco en notas periodísticas como *"supuesto autor del hackeo de los sistemas de la Policía Federal"* (Telam, 8 de octubre de 2019[1]) y hasta como *"la persona que orquestó el ataque" y "el principal investigado en el caso"* (Clarín, 8 de octubre de 2019[2]).

Que esta serie de atropellos ha lesionado mi derecho a trabajar *(****artículo 23*** *de la Declaración Universal de Derechos Humanos)* por partida doble: ¿quién en su sano juicio confiaría el control de sus sistemas informáticos y de su información sensible a un profesional sobre el que recae semejante sospecha, ya que las noticias antedichas aparecen entre los primeros resultados al buscar mi nombre mediante cualquier buscador de la web? (Ver notas de Todo Noticias[3], Perfil[4], La Nación[5], Ámbito Financiero[6] y La Voz del Interior[7], por nombrar solo algunos medios de alcance nacional). Además, ¿quién convocaría como observador para garantizar la transparencia electoral a alguien sospechado de liderar una banda criminal?

Que este limbo procesal en el que me han colocado se hace insoportable con el paso de cada día. No puedo defenderme de lo que no se me acusa, y sin embargo sigo presente en el expediente. Esto lesiona gravemente mi derecho a la defensa *(****artículo 11*** *de la Declaración Universal de Derechos Humanos).* No puedo dejar de preguntarme cuánto más deberé esperar para que alguien me diga cuál es mi situación procesal y de qué se me acusa en concreto.

Como ha dicho la Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal en la causa "LASKOWSKI. Patricia y otros s/ procesamiento" (SAIJ: FA07260115): "*De lo que se trata en la indagatoria, tal como llevamos dicho en otros precedentes (de esta Sala, causa n° 36.252 "CONSTANTINO", del 09/12/2004, reg. n° 1307; causa n° 39.759 "MÁRQUEZ MARTÍN"del 28/12/2006, reg. n° 1439), es de otorgar al imputado la posibilidad de pronunciarse en el proceso en condiciones que aseguren que esa declaración sea un acto de defensa. No podrá afirmarse que "escuchar al imputado" garantiza su derecho de defensa si no*

1 https://www.telam.com.ar/notas/201910/398367-detenido-experto-informatica-hackeo-policia-federal.html
2 https://www.clarin.com/policiales/detienen-informatico-filtracion-datos-policia-federal_0_wyaOw6Xp.html
3 https://tn.com.ar/policiales/detuvieron-un-informatico-por-filtracion-de-datos-en-twitter-de-la-policia-federal_1000786/
4 https://www.perfil.com/noticias/politica/detuvieron-experto-informatico-javier-smaldone-causa-hackeo-policia-lagorraleaks.phtml
5 https://www.lanacion.com.ar/tecnologia/varios-detenidos-robo-datos-del-sistema-informatico-nid2295293
6 https://www.ambito.com/informacion-general/allanamientos/detuvieron-unas-horas-experto-informatico-hackeo-policia-federal-n5058871
7 https://www.lavoz.com.ar/politica/gorraleaks-demoraron-al-informatico-javier-smaldone

existe, entre otras circunstancias, algo de qué defenderse (imputación) y el conocimiento de esa imputación correctamente deducida (intimación). Este último extremo lo reglamenta el art. 298 del Código Procesal Penal de la Nación al establecer la obligación del juez de informar "detalladamente al imputado el hecho que se le atribuye".

Dicho fallo se apoya en lo expresado por Julio Maier: *"Como se trata de hacer conocer la imputación, el acto por el cual se la intima debe reunir las mismas calidades que advirtiéramos para aquélla; debe consistir, así, en la noticia íntegra, clara, precisa, y circunstanciada del hecho concreto que se atribuye al imputado. No se cumple esta condición de validez si sólo se advierte sobre la ley penal supuestamente infringida, o se da noticia del nomen iuris del hecho punible imputado, o se recurre, para cumplir la condición, a conceptos o abstracciones que no describen concretamente la acción u omisión atribuida, con todas las circunstancias de modo, tiempo y lugar que la definen como un comportamiento singular de la vida del imputado…"* (Maier, Julio B. J., "Derecho Procesal Penal argentino", Del Puerto, Buenos Aires, 1996, T. 1, p. 560).

Precisamente, lo único que se me ha notificado a modo de imputación es lo que aparece en la orden librada por V.S. a fs. 623, que dice que el allanamiento fue dispuesto *"en relación al expediente CCC 55276/2019 caratulado "N.N. s/ violación de correspondencia... ""*, y *"con la finalidad de proceder al secuestro de telefonía celular. elementos informáticos, dispositivos de almacenamiento, anotaciones y registros vinculados a la maniobra investigada en los autos de referencia - maniobras de "hackeo" a la Policía Federal Argentina, Prefectura Naval Argentina y Policia de la Ciudad, durante el mes de julio de 2019 y difusión del material obtenido. por parte un usuario de la red social twitter "@lagorraleaks" bajo el lema "LaGorraleaks 2.0"-"*. Tampoco me dio mayores detalles sobre la imputación en mi contra el acta de detención de fs. 738, en la cual se me leyeron los artículos 73, 104, 107, 197, 199, 258, 279, 294, 295, 296 y 298 del Código Procesal Penal de la Nación.

II

Que entre los elementos secuestrados en el allanamiento realizado en [redacted] se encontraban dos (2) notebooks: una marca Asus de mi propiedad y otra marca Dell propiedad de [redacted]. Ambas computadoras fueron envueltas en papel film transparente sellado este con una única faja de secuestrado.

Que el formulario único de cadena de custodia de fs. 1116 en el ítem "descripción de los efectos" dice: *"UNA (01) NOTEBOOK MARCA ASUS MODELO* [redacted]*, N° SERIE* [redacted]*. UNA (01) NOTEBOOK MARCA DELL CON NÚMERO* [redacted] *Y*

S/N [redacted]”, en tanto que en “descripción del envase o envoltorio para traslado” puede leerse “PAPEL FILM TRANSPARENTE”.

Que la certificación de elementos recibidos de fs. 1124-1129 dice: *“Dos Notebook negras envueltas en papel film cerrado con faja de secuestro y pegadas con cinta adhesiva, y un papel pegado de color blanco que dice ‘Notebook Smaldone’ y el formulario único de cadena de custodia que señala y describe las notebooks una marca Asus y otra marca Dell, del domicilio* [redacted]*”*.

Que el 21 de enero de 2021 la Fiscalía Nacional en lo Criminal y Correccional Federal N° 1 entregó a [redacted] su notebook Dell, ya separada de la notebook Asus de mi propiedad, exhibiéndole además esta última (se ajuntan al final del presente escrito fotografías de ambos elementos, tomados por [redacted] en dicha oportunidad).

Que en el recibo firmado por [redacted] el 21 de enero de 2021 dice que le fue entregada: *“Una notebook marca Dell, nro. de serie* [redacted] *y s/n* [redacted]*, que vino con el mismo acta de cadena de custodia que la notebook que se encuentra reservada en la Fiscalía y sin faja de secuestrado”*.

Que no se ha realizado el desdoblamiento de la cadena de custodia al separar los dos elementos remitidos dentro de un mismo envoltorio —un “film para embalaje” y no una bolsa con cierre hermético, tal como prescribe el “Protocolo unificado de los ministerios públicos de la República Argentina” del Programa Nacional de Criminalística— y bajo un mismo formulario único de cadena de custodia.

Que todo esto fue hecho, además, sin notificarme de que se realizaría la apertura de un envoltorio conteniendo elementos de mi propiedad, por lo cual no pude ejercer el correspondiente control de parte en dicho acto irreproducible y definitivo.

Que lo expuesto contraviene lo expresado por la Sala 2 de la Cámara Criminal y Correccional Federal, que en su fallo del día 14 de febrero de 2020 (CFP 55276/2019/3/CA2) dijo: *“[…] frente a los elementos novedosos aportados por la parte al desarrollar sus agravios, una vez devuelta la causa a su origen incumbirá al Director del proceso disponer -de estimarlo necesario- el urgente análisis de la información contenida en los aparatos secuestrados y determinar si esta guarda -o no- concreta vinculación con los eventos pesquisados en el sumario.* ***Ello habrá de hacerse, claro está, bajo el estricto control de la defensa,*** *teniendo en cuenta que el interesado manifestó poseer en dichos dispositivos información asociada a investigaciones periodísticas propias* [redacted]*, y que es misión del Juez -en sintonía con los derechos de raigambre constitucional que se han invocado- garantizar tanto*

el resguardo de esos datos como de sus fuentes (ver CSJN, Fallos: 324:975, 248:291, entre otros, y de esta Sala II, CFP 7129/18/1/CA1, reg. 47.997 del 5/09/19 y sus citas)”. (El resaltado es añadido por esta parte).

Que por esto pongo en conocimiento de V.S. que se ha violado la integridad de mi computadora, no pudiendo garantizarse que su contenido no haya sido manipulado de alguna manera. De esta forma, cualquier peritaje que pudiera realizarse sobre este elemento resultará nulo, de nulidad absoluta. De la misma manera, al no haber podido ejercer el control de parte sobre el acto de apertura realizado, tampoco puedo estar seguro de que no se ha violado la confidencialidad de los datos contenidos en mi computadora.

III

Que en el escrito que consta a fs. 1157-1161, que fuera presentado por esta parte el 16 de octubre de 2019, se señala la afirmación falaz introducida por el subcomisario Carlos Alberto Aguirre, al sindicarme como sospechoso del hecho investigado en esta causa, afirmando que fui hallado culpable del “hackeo” a la ministra Patricia Bullrich y el Ministerio de Seguridad, ocurrido en enero de 2017.

El día 13 de agosto de 2019 el subcomisario Claudio Ricardo Ramos, 2do Jefe a cargo de la División Investigación de Delitos Tecnológicos de la Policía Federal Argentina declaró —en presencia del subcomisario Carlos Alberto Aguirre, jefe de la División Investigaciones de Delitos Tecnológicos, y el comisario Ricardo Rubén Rochas, jefe del Departamento de Ciber Delito de la misma fuerza— que: *“teniendo en cuenta la modalidad y tipografía utilizadas por el usuario de Twiter '@lagorraleaks2.0' se lo puede relacionar con las personas que en el año 2017 hackearon la cuenta de la Ministra Patricia Bullrich, llamados R.D.M.M., que utilizaba cono usuario "Niño orsino" y E.V.C., más aún cuando el propio usuario "@lagorraleaks2.0" hizo mención en este último episodio por la red social Twiter que precisamente ahora volcaría la información de la Policia Federal de la misma forma en la que en el año 2017 habia hecho respecto de la Ministra. Que según cree por aquel hakeo los nombrados fueron oportunamente condenados”* (fs. 31-32). Como ya fue dicho, la causa en la que se investigan estos sucesos tiene como procesados a R.D.M.M. y a E.V.C, pero aún no se ha sustanciado el juicio oral.

El día 15 de agosto de 2019 —solo dos días después de la declaración del subcomisario Ramos, en la que se encontraba presente— el subcomisario Aguirre reiteró estos dichos, con el agregado de mi nombre: *“habiéndose comprobado la autoría de los autores involucrados en el hecho del hackeo a la cuenta de Twitter de la Ministra en el año 2.017, y la capacidad técnica que estos presentan para llevar a cabo los presentes hechos, y habiendo encontrando publicaciones donde se adjudican estos al mismo tiempo, se considera a estos como posibles*

responsables del hecho, tratándose de las siguientes personas: R.D.M.M. [...] E.V.C [...] JAVIER SMALDONE” (fs. 67-68).

Lo que dijo Aguirre es falso: no solo no se había comprobado la autoría de los hechos ocurridos en 2017, sino que nunca fui imputado por haber tenido participación alguna en los mismos. De hecho, y como fue acreditado a fs. 1162-1164, en dicha causa espontáneamente presenté prueba y me fue tomada declaración testimonial. Además el subcomisario tampoco mostró cuáles eran las supuestas publicaciones donde alguien me adjudicaba el hecho ahora investigado, por la sencilla razón de que nunca existieron. Finalmente, cometió un error revelador al referir que en las investigaciones del hecho de 2017 *“se hace referencia a un **tercer** involucrado en dicha maniobra bajo el usuario @[redacted]”*. Según su enumeración anterior —donde insertó mi nombre, cuando dos días antes había convalidado los dichos de Ramos en los que no se me mencionaba— este involucrado no sería el tercero sino el cuarto.

Es también llamativo que desde la ocurrencia del *“phishing”* mediante el cual supuestamente fueron comprometidas 3 cuentas de Gmail de la Policía Federal, el 28 de julio de 2019, los investigadores policiales analizaron las direcciones IP desde las cuales se había accedido a las mismas, pero en ningún momento prestaron atención al programa utilizado para llevar a cabo el engaño ni a su ubicación. Y es que resulta notable —y es repetido varias veces en los informes policiales de fs. 21-72, entre otros— que el programa malicioso *“login.php”* había sido alojado en un servidor de la propia Superintendencia de Bienestar *“www.supbienestar.gob.ar”* —desde donde parece haberse originado gran parte de la información luego filtrada:

https://**www.supbienestar.gob.ar**/2018/documentacion/acceso/**login.php**

Cualquier informático que investigue una maniobra de este tipo se preguntaría inmediatamente cómo fue que los atacantes tuvieron acceso suficiente para poner allí el programa malicioso, y acto seguido procedería a analizarlo para saber hacia dónde enviaba los datos obtenidos a través del engaño. Pero nada de esto es informado por el personal de la División de Investigación de Delitos Tecnológicos de la Policía Federal en los informes posteriores a la denuncia, ya que no hay ni siquiera una captura de pantalla de este elemento central en la maniobra investigada. Cuesta imaginar cuál puede haber sido la motivación para omitir un elemento de tal relevancia, que pone de manifiesto la ocurrencia de un hecho anterior al denunciado y posteriormente investigado: el acceso ilegítimo a un servidor de la Superintendencia de Bienestar, su alteración, la introducción en el mismo de un programa destinado a causar daño y posiblemente el acceso a información alojada en el mismo.

Otro elemento imposible de omitir por un profesional informático es que, según la información periodística basada en fuentes policiales, el volumen de los datos filtrados iría entre los **250 y**

los 700 GB[89] (de los cuales **259 GB** se encuentran hoy publicados en la web, accesibles a cualquier persona[10]), en tanto que 3 cuentas regulares de Gmail —tal las denunciadas como origen de los mismos— no pueden almacenar más de **45 GB** en conjunto. Evidentemente la mayor parte de la información, si no toda, debió provenir de otro lugar (quizás, el propio servidor de la Superintendencia de Bienestar). Sin embargo, esto tampoco fue denunciado inicialmente.

Y durante los **quince (15) días** siguientes a la ocurrencia del *"phishing"* los investigadores nunca manifestaron sospechar ninguna vinculación entre este hecho y lo ocurrido en enero de 2017 con las cuentas de la ministra Patricia Bullrich y el Ministerio de Seguridad (ver informes de fs. 01-16 y fs. 21-27). Pero luego, a menos de 24 horas de producirse la filtración de datos —evento que cambió la magnitud del hecho en cuestión, agravándolo y haciéndolo de público conocimiento—, el personal policial rápidamente sindicó como sospechosos de toda la maniobra a quienes supuestamente habían realizado el *"hackeo"* anterior (sin aportar evidencia alguna y hasta incluyendo información falsa).

No es hasta el informe policial del **3 de septiembre de 2019**, que consta a fs. 236-243, que se reconoció —aunque de forma bastante confusa— que el servidor de la Superintendencia de Bienestar había sido vulnerado con anterioridad a la maniobra de *"phishing"*, y que parte de la información filtrada fue obtenida de este. En dicho informe el subcomisario Aguirre dijo que *"como medida de seguridad informática institucional, técnicos idóneos procedieron a proteger los servidores afectados lográndose el resguardo del registro de los Logs de conexión al servidor, de los correos electrónicos, del Firewall y de los archivos denominados LOG.TXT donde se guardaban los usuarios y contraseñas de quienes habrían ingresado y habrían sido direccionados por el Phishing; realizando una copia de toda la información impactada en soporte óptico, con la finalidad de preservar la huella digital dejada por el atacante, quien podrÍa borrarla mediante un acceso remoto"*. Por encima de la redacción confusa podemos entender que afirma que se resguardaron tanto el archivo donde el programa malicioso almacenaba las contraseñas obtenidas (LOG.TXT), como así también los registros (logs de conexión al servidor y firewall) que permitirían obtener las direcciones IP desde las cuales se accedió al primero. Pero, insistimos, esto no fue dicho en la denuncia y los informes iniciales sino solo después de ocurrida la filtración, y tampoco es mencionado en ninguno de los informes policiales posteriores incluidos en el expediente.

El día **5 de febrero de 2020** la Agencia de Acceso a la Información Pública, en su resolución RESOL-2020-30-APN-AAIP[11], dijo: *"Que en relación con la vulnerabilidad producida en el*

8 https://www.infobae.com/sociedad/policiales/2019/08/16/la-gorra-leaks-que-hay-en-los-archivos-secretos-de-la-policia-filtrados-por-hackers/
9 https://www.lanacion.com.ar/seguridad/estuve-varios-meses-accediendo-red-policia-federal-nid2277390/
10 https://[redacted]
11 https://www.argentina.gob.ar/sites/default/files/rs-2020-30-apn-aaip.pdf

servidor del aplicativo ‘https://supbienestar.gob.ar’, la investigada manifestó mediante informe N° IF-2019-80081802-APN-SCIB#PFA que: ‘la información (vulnerada) fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmail’”. Esto es la Policía Federal Argentina reconociendo —siempre después de ocurrida la filtración y nunca antes— que la información fue obtenida mediante el acceso ilegítimo a un servidor de la Superintendencia de Bienestar. Una historia muy diferente a la relatada en la denuncia inicial y sostenida durante los primeros días.

En lo que a esta parte respecta, luego siguió el rocambolesco informe policial de fs. 515-532 que fue oportunamente analizado y descalificado a fs. 1159-1160, y que básicamente se resume en sospechas basadas en mis conocimientos técnicos, mis opiniones políticas y diálogos inocentes y públicos sacados de contexto.

A fs. 626 notamos que la Procuraduría de Investigaciones Administrativas ha solicitado vista de esta causa en el marco del expediente PIA Nro. 534/19. A fs. 1406 se observa que dicha procuraduría ha enviado un oficio a la Policía Federal solicitando *“la producción de pormenorizado informe, indicando la totalidad de actuaciones iniciadas, cuyo objetivo fuera investigar la presunta vulneración de las bases informáticas de ela POLICÍA FEDERAL ARGENTINA, y posrerior publicación de aproximadamente 700 gigabytes de información, a través del usuario/temática conocida públicamente como "La Gorra Leaks" acontecida en Agosto de 2019”*. Estimamos que dicho expediente puede contener información valiosa para echar luz sobre cómo fue realizada esta oscura investigación policial.

IV

Pido a V.S. se formule una imputación en mi contra y acto seguido se me tome declaración indagatoria, dándome así la posibilidad de defenderme. Y en caso de que resulte imposible formular una acusación concreta y real contra mi persona —tal y como vengo sosteniendo desde un principio, dado que ni siquiera había razón fundada para allanar mi domicilio— dicte mi sobreseimiento en esta causa y me devuelva mis herramientas de trabajo y mis datos, cesando de una vez en la vulneración de mis derechos fundamentales. Ya sea en cualquiera de los dos sentidos, pido que de una buena vez se resuelva mi situación procesal en esta causa: dieciséis (16) meses han sido más que suficientes.

También pido se impugne el uso del contenido de mi notebook marca Asus como medio de prueba.

Reitero además el pedido de devolución de mis herramientas de trabajo, que contienen información de vital importancia para mi actividad profesional.

Finalmente solicito se dé impulso procesal a mi pedido realizado a fs. 1161 —detallado en el presente escrito aludiendo siempre a fojas anteriores del expediente, y al que adhirieron organizaciones no gubernamentales de más de 10 países en el comunicado de fs. 1411-1412— de que investigue por qué el personal policial, encabezado por el subcomisario Carlos Alberto Aguirre, me introdujo en la presente investigación, valiéndose para ello de información objetivamente falsa. Además, pido se investiguen las notorias omisiones en la investigación de los hechos acontecidos.

IV

En razón de lo expuesto, de V.S. solicito:

1 Se expida precisando mi situación procesal.
2 Se formule imputación en mi contra y se me tome declaración indagatoria o, en su defecto,
3 se dicte mi sobreseimiento en esta causa.
4 Se impugne el uso del contenido de mi notebook como medio de prueba.
5 Se me devuelvan los elementos de trabajo que me fueran secuestrados.
6 Se ordene la correspondiente extracción de testimonios a los fines de investigar los ilícitos y omisiones cometidos por el personal policial.
7 Se solicite a la Procuraduría de Investigaciones administrativas el expediente PIA Nro. 534/19 ad effectum videndi et probandi.
8 Se solicite a la Policía Federal Argentina los sumarios internos relacionados a esta investigación ad effectum videndi et probandi.

Tener presente lo expuesto, SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

Notebook marca Dell devuelta a [redacted]

Notebook marca Asus, propiedad de Javier Smaldone, exhibida a [redacted] *en la fiscalía*

AMPLÍA – REITERA – SOLICITA

Señor Fiscal Federal:

Javier Lorenzo Carlos Smaldone, DNI N.º [redacted], con el patrocinio de mi abogado defensor Pablo Slonimsqui, en autos caratulados "N.N. Y OTROS S/VIOLACIÓN DE CORRESPONDENCIA, INTIMIDACIÓN PUBLICA Y VIOLACIÓN SIST. INFORMÁTICO ART. 153 BIS 1° PÁRRAFO DENUNCIANTE: LA ROCCA, MARIO Y OTROS", expediente Nº 55276/2019 que tramitan ante el Juzgado Nacional en lo Criminal y Correccional Federal N° 9, Secretaría N° 18, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), respetuosamente digo:

AMPLÍA

Que en el escrito presentado en fecha 1 de marzo de 2021 por esta parte se hicieron notar las llamativas omisiones de la denuncia presentada el 30 de julio de 2019 por personal de la Policía Federal sobre los hechos de marras, que se limitó a manifestar la vulneración de tres (03) cuentas de Gmail en uso por dicha fuerza. En dicho escrito se destacó que el acceso indebido al servidor *supbienestar.gob.ar* de la Superintendencia de Bienestar y su posterior modificación para realizar una maniobra de *"phishing"* no fueron reconocidos sino hasta luego de producida la filtración masiva de datos el 12 de agosto de 2019, conocida popularmente como *"La Gorra Leaks 2.0"*. También se hizo alusión a la resolución RESOL-2020-30-APN-AAI de la Agencia de Acceso a la Información Pública[1], según la cual en el informe IF-2019-80081802-APN-SCIB#PFA de la Policía Federal se reconocía que: "*la información (vulnerada) fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmail"*. Respecto de esto último es que quisiera darle algunas precisiones técnicas y consideraciones con la esperanza de contribuir a su mejor comprensión de los hechos, desde mis más de veinticinco años de experiencia en la instalación, el mantenimiento y el soporte de servidores informáticos como los aquí involucrados.

El software PHP (un lenguaje de programación, de los más utilizados en la *World Wide Web*) en su versión 5.6.3 fue publicado el 14 de noviembre de 2014[2] (y la siguiente versión, 5.6.4, el 18 de diciembre de 2014). A mayo de 2016 ya existían al menos cuatro (04) vulnerabilidades graves detectadas, documentadas, publicadas y explotables[3]. Esto significa que al momento de

1 https://www.argentina.gob.ar/sites/default/files/rs-2020-30-apn-aaip.pdf
2 https://www.php.net/releases/index.php
3 https://cvedetails.com/vulnerability-list.php?vendor_id=74&product_id=128&version_id=178179&order=3

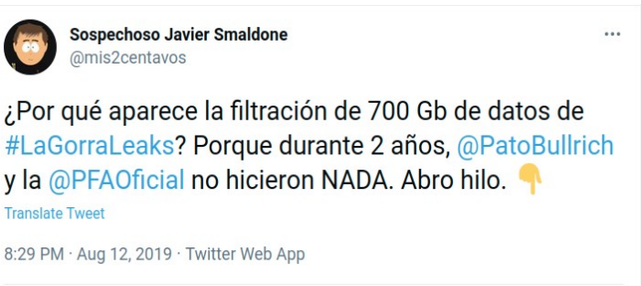
detectarse la intromisión en el servidor *supbienestar.gob.ar*, el 28 de julio de 2019, hacía ya más de tres años que cualquier persona con modestos conocimientos en la materia podría haber realizado una maniobra similar a la que, esta vez, tomó estado público.

Es realmente alarmante pensar que la institución policial alojaba información confidencial en un servidor en semejante estado de abandono. No se entiende cómo no se tomaron medidas para solucionar problemas de seguridad graves documentados y publicados en mayo de 2016. Bastaba para esto con una simple actualización del software PHP, tarea rutinaria para cualquier profesional en la materia y que no demanda más que unos minutos.

La aplicación de actualizaciones de seguridad es una tarea crucial en el mantenimiento de servidores, y es realmente crítica en el caso de aquellos expuestos a Internet (como es el caso de *supbienestar.gob.ar*). Es una práctica común y bien establecida en la industria la actualización de servidores de forma semanal o, a lo sumo, mensual. Y en el caso de publicarse vulnerabilidades graves (como las descubiertas en PHP 5.6.3 en mayo de 2016), debe realizarse tan rápido como sea posible. Por otra parte, cualquier administrador de sistemas de este tipo sabe que PHP es un constante vector de ataques (que ha posibilitado filtraciones de datos importantes, como la que nos ocupa) ya que regularmente se encuentran en él errores y vulnerabilidades que deben ser corregidas.

Es realmente alarmante que ni siquiera se revisara la seguridad de dicho servidor y se actualizara el componente de software defectuoso luego de que en mayo de 2017 se produjera la primera filtración de datos de la Policía Federal, conocida como *"La Gorra Leaks"*. En aquella ocasión esta parte contribuyó a denunciar el hecho ocurrido aportando prueba en el marco de la causa Nº 1033/2017 del Juzgado Nacional en lo Criminal y Correccional Federal Nº 2 y prestando luego declaración testimonial. Esto motivó una denuncia realizada por la Fiscalía Nacional en lo Criminal y Correccional N° 10 el 5 de junio de 2017. Quizás esto explique la animosidad puesta de manifiesto por los investigadores policiales hacia mi persona.

Tan pública y notoria fue la inacción policial ante el hackeo y posterior filtración de mayo de 2017 que, al tomar estado público la filtración ocurrida el 12 de agosto de 2019, expresé lo siguiente en la red social Twitter[4]:



4 https://twitter.com/mis2centavos/status/1161057262321983488

En dicho tweet —y en el hilo que de él se desprende— expliqué lo que hoy, a la luz de la evidencia resumida en este escrito, aparece claro: que la nueva filtración se produjo porque ni se investigó debidamente ni se tomaron las medidas de seguridad adecuadas luego de la primera filtración de información de la Policía Federal Argentina. Es notable que ni este tweet, ni los que le siguen a continuación, fueran citados ni por los informes policiales de "ciberpatrullaje" de fs. 199-231 —donde aparecen once (11) tweets míos emitidos por esos días— ni en el "ANEXO 4" de fs. 515-532, exclusivamente dedicado a mi persona —donde aparecen cincuenta y siete (57) tweets míos emitidos en distintos momentos a lo largo de más de ocho (08) años.

Dado que tanto al realizar la denuncia como al ratificarla se ocultó lo sucedido con el servidor *supbienestar.gob.ar,* y solo se reconoció luego de hacerse evidente al tomar estado público el contenido de los archivos filtrados, cabe preguntarse además si este fue el único servidor vulnerado en dicha oportunidad y cuántos otros se encontraban en similar estado de incuria.

Es llamativo también que en ningún informe policial incluido en el expediente muestre que se haya analizado en detalle la naturaleza de la información filtrada, ni siquiera su volumen, lo que resultaría esencial para determinar el origen de la misma y el impacto y posibles consecuencias de los hechos ocurridos.

Para finalizar, recordemos que la Agencia de Acceso a la Información Pública en la resolución del 5 de febrero de 2020 antes citada aplicó sendos apercibimientos a la Policía Federal Argentina por haber incumplido los deberes de seguridad (artículo 9) y de confidencialidad (artículo 10) de la Ley N° 25.326.

En definitiva:

- El servidor *supbienestar.gob.ar* de la Superintendencia de Bienestar de la Policía Federal tenía un componente de software sin actualizar (PHP) aproximadamente desde **diciembre de 2014**.
- Dicho software tenía vulnerabilidades graves que eran públicas desde **mayo de 2016**.
- Desde ese momento, cualquier persona con mínimos conocimientos podía explotar dichas vulnerabilidades y acceder a la información confidencial alojada en el servidor.
- No se tomaron medidas para solucionar dichas vulnerabilidades luego de ocurrida la filtración de datos de la Policía Federal (*"La Gorra Leaks"*) en **mayo de 2017**.
- Dichas vulnerabilidades seguían presentes en el servidor y fueron explotadas para realizar una maniobra de *"phishing"* (que derivó en el compromiso de tres cuentas de correo electrónico) el **28 de julio de 2019**.
- No se hizo referencia alguna a estas vulnerabilidades, ni al acceso ilegítimo al servidor *supbienestar.gob.ar*, ni alteración del mismo, en los informes policiales previos a la

denuncia realizada por la Policía Federal de forma telefónica el **30 de julio de 2019** (fs. 17) y ratificada en el juzgado el **13 de agosto de 2019** (fs. 31-32).

- En la denuncia inicial el personal policial dijo que los datos filtrados (*"La Gorra Leaks 2.0"*) —entre 259 GB y 700 GB, según las fuentes periodísticas— provenían de tres (03) cuentas de Gmail comprometidas, que en conjunto pueden almacenar solo 45 GB.
- La Policía Federal dijo a la Agencia de Acceso a la Información Pública que la filtración se produjo por la vulneración del servidor *supbienestar.gob.ar,* debida a los problemas de seguridad del software PHP no solucionados, y que la información (vulnerada) fue obtenida del mismo. Fue sancionada por esta última el **5 de febrero de 2020**.

REITERA - SOLICITA

En razón de lo expuesto, reitero mi pedido de que se investiguen las notorias omisiones por parte de la Policía Federal Argentina en la denuncia y la investigación de los hechos acontecidos.

Pido también se solicite a la Agencia de Acceso a la Información Pública el expediente EX-2019-72366951- -APN-DNPDP#AAIP, que motivara la resolución RESOL-2020-30-APN-AAIP, incluyendo el informe IF-2019-80081802-APN-SCIB#PFA aludido en la misma ad effectum videndi et probandi.

Además, solicito se extraigan testimonios de la causa Nº 1033/2017, que tramita en el Juzgado Nacional en lo Criminal y Correccional Federal Nº 2, a fin de determinar si a raíz de la filtración ocurrida y denunciada en mayo de 2017 se emitieron alertas a la Policía Federal respecto del nivel de seguridad de sus servidores y qué medidas tomó la fuerza policial en consecuencia.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

MANIFIESTA – SOLICITA

“Como antes y como ahora —y como en casi todos los tiempos— cuando llega la noche, la gente se va a dormir. Algunos lo hacen donde no deben y por las razones equivocadas, lejos de sus hijos y de sus familias. Otros, con más suerte y menos injusticias sufridas, pueden hacerlo al amparo de sus hogares. Y algunos otros seguramente no pueden dormir pensando en todas las cosas malas que han hecho.”

(Enrique Piñeyro, “El Rati Horror Show”, 2010)

Señor Fiscal Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], con el patrocinio de mi abogado defensor Pablo Slonimsqui, en autos caratulados “N.N. Y OTROS S/VIOLACIÓN DE CORRESPONDENCIA, INTIMIDACIÓN PÚBLICA Y VIOLACIÓN SIST. INFORMÁTICO ART. 153 BIS 1° PÁRRAFO DENUNCIANTE: LA ROCCA, MARIO Y OTROS”, expediente Nº 55276/2019 que tramitan ante el Juzgado Nacional en lo Criminal y Correccional Federal N° 9, Secretaría N° 18, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), respetuosamente digo:

MANIFIESTA

Que el 19 de marzo del corriente recibí respuesta a un pedido a la Agencia de Acceso a la Información Pública, en la que se me remitió el contenido completo del expediente EX-2019-72366951- -APN-DNPDP#AAIP, que motivara la resolución RESOL-2020-30-APN-AAIP en la que la Dirección Nacional de Protección de Datos Personales (DNPDP) sancionó a la Policía Federal Argentina por la indebida protección de datos sensibles. Dicho expediente incluye el informe policial IF-2019-80081802-APN-SCIB#PFA (fechado el **4 de septiembre de 2019**), que anteriormente pedí a usted solicitara a la citada agencia, el cual adjunto como anexo al presente escrito y del que a continuación resalto algunos pasajes, contrastándolos con lo expresado —y lo omitido— por la fuerza policial en el expediente de marras.

Ante la requisitoria de la DNPDP: *“1.- Indicar desde cuando se tiene conocimiento de la filtración de los datos y que medidas fueron adoptadas en consecuencia”*, la Policía Federal dijo:

> “Posteriormente, y ya teniendo identificado el tipo de información filtrada, la Sección CIBERSEGURIDAD estableció en principio, que unos de los vectores de ataque correspondieron a la intrusión de los ciberdelincuentes a diversas casillas de correos comerciales (Hotmail, Gmail) utilizadas por las dependencias policiales, mediante una

> técnica de Phishing que fuera detectada, reportada por esta Sección y mitigada con fecha 30/07/2019, por la Sección INFORMATICA de la Superintendencia de BIENESTAR, en razón de que en el sitio de la Página Oficial https://supbienestar.gob.ar se encontraba alojado un formulario malicioso que simulaba ser de un acceso al servicio de Onedrive para la descarga de un archivo, técnica utilizada por el ciberdelincuente para apoderarse de los nombres de usuarios y contraseñas de acceso [...]"

Según esto, la Superintendencia de Bienestar de la Policía Federal habría detectado y mitigado la existencia de un formulario malicioso en uno de sus servidores el día **30 de julio de 2019**. Como ya se hizo notar en múltiples presentaciones anteriores de esta parte, nada de esto fue mencionado ni en los informes presentados junto a la denuncia telefónica del subcomisario Claudio Ricardo Ramos **de ese mismo día** (fs. 17), ni en su declaración del **13 de agosto de 2019** (fs. 31-32).

> "En este contexto, el día martes 13 de agosto, se conformaron equipos de trabajo permanentes integrados por profesionales en la materia de ciberseguridad, peritos informáticos, analistas de sistemas y técnicos, entre otros. Dentro de las divisiones de tarea, se crearon grupos de análisis de la información, sanitización de equipos y redes informáticas, detección y alerta temprana de incidentes, y de contacto para evacuar cualquier tipo de consultas relacionadas con seguridad de la información para todas las dependencias policiales, que así lo requerían".

¿Por qué se crearon esos equipos de trabajo el **13 de agosto de 2019**, cuando los ataques se denunciaron el **30 de julio de 2019**? ¿Cuál era el "contexto", el ciberataque y la fuga de información, o que los mismos hubieran tomado estado público el día anterior? Llamativamente **el mismo día**, en la declaración que consta a fs. 31-32, la policía ya sindicaba a dos sospechosos y solo **dos días después**, a fs. 67-68, a un tercero (esta parte), sin haber realizado ninguna investigación del incidente o por lo menos sin declarar haberla hecho.

> "El día miércoles 14 de agosto, se conformó una reunión del COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, integrada por Oficiales Superiores y Jefes de las principales áreas específicas, donde se expuso entre los presentes los hechos de conocimiento público, a los fines de analizar la cuestión y realizar recomendaciones para mitigar estos sucesos. En esa inteligencia, el Comité elaboro un documento "Normas de Seguridad Informática" con reitero de objetivos inmediatos y a futuro que eviten la fuga de información Institucional."

¿Por qué se tomaron **quince días** para crear este comité? ¿Qué sucesos intentaban mitigar ¿La vulneración de sus servidores y la fuga de información, o su conocimiento público?

Ante la requisitoria de la DNPDP: *"2.- Informar cuales fueron las fallas de seguridad que posibilitaron dichas filtraciones"*, la Policía Federal dijo que según la Superintendencia de Bienestar:

> "El día 31 de Julio de corriente año se tomó conocimiento a través de un llamado telefónico del Subcrio VITTUZI, jefe de le Sección Ciberseguridad de la Superintendencia Federal de la Información y las Comunicaciones, de un e-mial enviado de la casilla div.supbienestar@hotmail.com (ajena a esta superintendencia) invitando a los usuarios a ingresar y completar un formulario alojado en nuestra web (www.supbienestar.gob.ar) con el fin de descargar un archivo. El mismo se trataba de un formulario fraudulento que simulaba ser el loguin de One Drive. Inmediatamente se procedió a eliminarlo de nuestra página ya que se comprobó que estaba recopilando correos y contraseñas en forma malintencionada."

Según esto, la Superintendencia de Bienestar afirma haber tomado conocimiento del formulario malicioso alojado en su servidor el día **31 de julio de 2019**, cuando la denuncia telefónica de la Policía Federal fue realizada **el día anterior**. Además, de las constancias obrantes a fs. 05-09 del expediente, se desprende que dicha repartición fue notificada de la situación por múltiples vías el **29 de julio de 2019**, pero a fs. 03-04 aparece un correo electrónico de alerta que fue enviado a la Superintendencia de Bienestar el **25 de julio de 2019**. Esto también contradice lo expresado anteriormente en el informe, donde se afirma que la vulnerabilidad en el servidor de la Superintendencia de Bienestar fue mitigada el día **30 de julio de 2019**.

.

> "El día 12/08 se nos alertó de un 'Hacker' que había publicado información personal de los afiliados de esta Policía Federal en la Deep Web. De inmediato se corroboró de dónde provenía dicha información. Se trata de datos del personal que se obtuvo en formato ".pdf" de los afiliados de la obra social fue realizada mediante un sistema de consulta que fue desarrollado por esta sección (https://portal.supbienestar.gob.ar/gestion_angel)."

Esta información es inédita, ya que nunca fue mencionada en ninguna denuncia ni informe policial. Según esto, las fichas del personal filtradas (en archivos PDF) se habrían extraído de un sistema presumiblemente llamado "Gestión Angel", ubicado en uno de sus servidores (`portal.supbienestar.gob.ar`), **que parecer ser diferente del primero en ser vulnerado** (`www.supbienestar.gob.ar`). Cabe preguntarse entonces a cuántos servidores de la Superintendencia de Bienestar tuvo acceso el atacante.

> “Notamos que la descarga del padrón no se realizó a la fuerza si no que, por el contrario, el ingreso se estableció con usuario y contraseña validos dentro del mismo, las descargas comenzaron el 12 de agosto de 2019 a las 01:15 am en adelante desde la ip de origen 93.188.163.28 que se encuentra asignada al proveedor Hostinger International y a su vez la ip se localizó en la cuidad de Greenville de carolina del sur (E.E.U.U.).”

Esto tampoco fue dicho en el expediente de marras. En este expediente solo hay una mención confusa a la empresa Hostinger a fs. 238 y un pedido del **5 de septiembre de 2019** (un día después del informe que estamos analizando) donde “se solicita a S.Sa. la autorización para la autorización de evidencia digital referente y relacionada con la cuenta asociada al servicio VPS Hostinger correspondiente a la IP 93.188.163.28", sin dar mayores precisiones ni fundamentar de dónde se obtuvo esa dirección IP.

Que el **12 de agosto de 2019** el atacante aún tuviera acceso a este sistema de la Superintendencia de Bienestar y procediera a descargar los archivos muestra claramente que las medidas supuestamente tomadas el **31 de julio de 2019** fueron completamente insuficientes.

> “Por otra parte, se habían publicado contraseñas de muchos mails institucionales de esta superintendencia y pudimos concluir que esta información fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmamil. Se estableció que se aprovechó de la información obtenida para poder conseguir acceso a mencionado portal del cual se obtuvo la información publicada.”

La Policía Federal tampoco ha mencionado en esta causa la publicación de contraseñas de correos electrónicos institucionales, hecho que reconoce en este párrafo. Respecto del disparate de tener en **julio de 2019** un servidor con una versión del software PHP de **noviembre de 2014**, esta parte ya se explayó abundantemente en su presentación anterior. Sin embargo debemos insistir en lo que aquí se dice claramente: que gran parte de la información filtrada y luego publicada no provino de las 3 cuentas de correo electrónico de Gmail vulneradas, tal como denunció la policía, sino del acceso ilegítimo al servidor de la Superintendencia de Bienestar, específicamente —según se agrega ahora— al sistema “Gestión Angel”. Y según se expresa, el usuario y la contraseña utilizados para esta maniobra habrían estado almacenados en el servidor de manera insegura. Otro despropósito.

El informe de la Policía Federal sintetiza la respuesta al punto “2” de la requisitoria de la DNPDP diciendo:

> “Reunida parte de la información y de acuerdo a las intervenciones del personal técnico de esta Sección, visualizando la información subida por los ciberdelincuentes a la Internet profunda (Deep Web) se puede concluir que las fallas que posibilitaron la filtración de los datos, son atribuidas en un principio al aprovechamiento y explotación de una vulnerabilidad del servidor web administrado por el área de Bienestar lo que ocasionara el alojamiento de un formulario malicioso para ser utilizado mediante la técnica de ingeniería social (Phishing) y obtener las credenciales de acceso a las cuentas de correo no institucionales utilizadas por las dependencias de la esta Policía Federal Argentina y el robo de las fichas en formato ‘.PDF’ de los afiliados a la obra social.”

La Policía Federal expresa aquí claramente lo que parece ser la realidad de los hechos. Ojalá lo hubiera hecho antes y con tanta precisión en la denuncia y los informes presentados a la Justicia.

Pero siguiendo con el informe, nos encontramos con otro dato revelador:

> “[...] tras el análisis de esta Sección CIBERSEGURIDAD de los archivos de la Deep Web, se determinó que gran parte de los archivos que se filtraron corresponde a información almacenada en tres terminales informáticas utilizadas por la División PESONAL SUPERIOR, las cuales pudieron haber sido comprometidas por el Ciberdelincuente con una infección de malware que permitiera el acceso total a los datos allí alojados en los discos rígidos, ya que se corroboró que esta Dependencia no utilizaba el almacenamiento de datos en la nube.”

Así es que, según esto, la información filtrada provino además de **tres (03) computadoras** de la División Personal Superior de la Policía Federal, que también fueron atacadas exitosamente como parte de la misma maniobra denunciada. A buena hora nos enteramos —pero lamentablemente, no por información aportada en esta causa por la policía.

Livianamente se habla de una posible infección de *“malware”* (software malicioso o virus informático). ¿Cómo es que tampoco se dijo nada de esto en la denuncia ni en ningún informe? Y lo más grave: ¿cómo es que no se investigó en profundidad si en efecto el delincuente introdujo software malicioso en esas computadoras policiales y qué otros dispositivos pudo haber infectado? Esto podría constituir un hecho gravísimo, ya que el atacante podría haber accedido a información mucho más allá de la que terminó siendo filtrada, e incluso tener acceso a la red de la Policía Federal quién sabe por cuánto tiempo.

> “Cabe aclarar que la División OBTENCION DE EVIDENCIA DIGITAL del Departamento CIBERDELITO, realizó imagen forense de los discos afectados y se encuentra en etapa de análisis e investigativa, causa que pasara al fuero Federal e

> interviniera el Juzgado Nacional en lo Criminal y Correccional Federal N° 9 a cargo del Dr. Luis Osvaldo RODRIGUEZ, Secretaría N° 18 del Dr. Juan Manuel GRANGEAT. Causa N° C-55276/19 Caratulada 'N.N S-VIOLACION DE CORRESPONDENCIA'"

Sería bueno que la Policía Federal, habiendo transcurrido ya **más de un año y medio**, aportara en este expediente los resultados de los peritajes realizados sobre las imágenes forenses de los discos afectados y, mejor aún, copias de estas últimas para poder ser peritadas con control de las partes intervinientes en este proceso penal.

Cabe recordar en este punto que en el informe del **3 de septiembre de 2019** —justo un día antes la respuesta a la DNPDP— firmado por el subcomisario Carlos Alberto Aguirre, que consta a fs. 236-243, se dice que el día 31 de julio de 2019 *"como medida de seguridad informática Institucional, técnicos idóneos procedieron a proteger los servidores afectados lográndose el resguardo del registro de los Logs de conexión al servidor, de los correos electrónicos, del Firewall y de los archivos denominados LOG.TXT donde se guardaban los usuarios y contraseñas de quienes habrían ingresado y habrían sido direccionados por el Phishing; realizando una copia de toda la información impactada en soporte óptico, con la finalidad de preservar la huella digital dejada por el atacante, quien podría borrarla mediante un acceso remoto, realizándose en forma inmediata la judicialización del hecho denunciado"*. A la luz de la respuesta policial al requerimiento de la DNPDP se entiende ahora que las copias realizadas serían de los discos del servidor de la Superintendencia de Bienestar (que aparentemente ahora serían dos (02) servidores), de las otras tres (03) computadoras vulneradas y del *"firewall"*. Pero ninguno de estos elementos fue aportado aún en la causa.

Ante la requisitoria de la DNPDP: *"3.- Detallar que tipo y cantidad de datos personales fueron comprometidos"*, la Policía Federal Argentina dijo:

> El área de Bienestar informó: Los datos comprometidos fueron: FICHAS PERSONALES DE LOS AFILIADOS, los cuales contienen los siguientes datos DNI, APELLIDO Y NOMBRE, N° AFILIADO, SEXO, ESTADO CIVIL, FECHA NACIMIENTO, EDAD, TELEFONO FIJO Y MOVIL, EMAIL, DIRECCIÓN, JERARQUIA, SITUACION REVISTA, LEGAJO PERSONAL, DEPENDENCIA, CBU, N° CAJA DE RETIRO, correspondiente a 220 Mil fichas. Asimismo, se divulgaron 1.083 cuentas de correo electrónico bajo el dominio @supbienestar.gob.ar con sus respectivas contraseñas. Los Directorios subidos en la Deep Web se identifican como "INFORMACION PERSONAL, OTRAS BASES DE DATOS".

Este párrafo aporta otra información valiosa —que tampoco aparece en el expediente de marras — al precisar la magnitud de la filtración y la naturaleza de los datos filtrados. La

Superintendencia de Bienestar reconoce el atacante accedió a **220.000 fichas con datos personales** y de **1.083 cuentas de correo con sus contraseñas** (el hecho de tener contraseñas almacenadas de forma insegura en un servidor es un despropósito descomunal cuyo análisis omitiremos de momento en honor a la brevedad).

Continúa la respuesta policial:

> "El área de Drogas Peligrosas: Informó que no pudo determinar a la fecha tipo y cantidad de datos personales, por no contar aún con la totalidad de la información compartida en internet.
> El área de personal: al día de la fecha no informó tipo y cantidad de datos filtrados. Hasta el momento esta Sección CIBERSEGURIDAD, no ha podido descargar para su análisis la totalidad de la información filtrada en la Deep Web, debido a que la tasa de transferencia para descarga en muy baja. No obstante, de lo que se desprende de lo visualizado existen gran cantidad de archivos de uso interno y administrativo de distintas dependencias, (.doc, pdf, xls, .rar , jpg, mp4, wav entre otros) que tuviera almacenados en los servicios de almacenamiento en la nube y los propios en discos rígidos internos ya anteriormente explicados."

Es realmente penoso que **veinte (20) días** no hayan sido suficientes para la Policía Federal Argentina para descargar los archivos filtrados. Lamentablemente, como ya fue dicho en una presentación anterior, otros sí lo hicieron y los replicaron en la World Wide Web, donde todavía pueden encontrarse *"googleando"*. Además, si **veinte (20) días** no fueron suficiente para descargarlos, ¿cuánto tiempo le tomó al atacante filtrarlos?

El informe policial finaliza:

> "Con respecto a la información filtrada en la Deep Web, desde el día Lunes 02 de septiembre del corriente año, no se encuentra disponible."

Si *googlearan*, aún transcurrido más de un año y medio, la encontrarían.

En resumen:

- El **25 de julio de 2019** una división de la Superintendencia de Drogas Peligrosas notificó a la Superintendencia de Bienestar de la recepción de un correo electrónico engañoso (*phishing*) que parecía provenir de esta última e incluía un enlace a un formulario malicioso alojado en uno de sus servidores (fs. 03-04).
- El subcomisario Ramos declaró —en presencia del subcomisario Aguirre y el comisario Rochas— que tomó conocimiento de la situación el **29 de julio de 2019** y que la

Superintendencia de Bienestar le informó que los correos electrónicos maliciosos habían llegado **en la mañana de ese mismo día**. (fs. 31-32).

- En su respuesta a la DNPDP, la Policía Federal informó que según la Superintendencia de Bienestar tomaron conocimiento de la maniobra realizada el **31 de julio de 2019** por un llamado telefónico del subcomisario Diego Hernán Vituzzi (pág. 7).
- A pesar de que en el contenido del correo electrónico engañoso se observa claramente que el servidor www.supbienestar.gob.ar había sido vulnerado, no se hizo mención alguna a este hecho hasta el **3 de septiembre de 2019** en el informe del subcomisario Aguirre (fs. 236-243) y el **4 de septiembre de 2019** en la respuesta de la Policía Federal a la DNPDP (págs. 1 y 7).
- Tanto en las constancias judiciales como en la respuesta de la Policía Federal a la DNPDP se observa una total inacción de esta fuerza entre los días **31 de julio y 12 de agosto de 2019**.
- Según su respuesta a la DNPDP, la Policía Federal conformó equipos de trabajo integrados por profesionales de ciberseguridad y otros expertos recién el **13 de agosto de 2019**, al día siguiente de haber tomado estado público la filtración "La Gorra Leaks 2.0" (pág. 2). Ese **mismo día**, el subcomisario Ramos en sede judicial —en presencia de Aguirre y Rochas— ya sindicaba como sospechosas a dos personas (fs. 31-32).
- En la respuesta de la Policía Federal a la DNPDP del **4 de septiembre de 2019** la fuerza reconoció que:
  - El atacante siguió teniendo acceso a los datos de la Superintendencia de Bienestar al menos hasta el **12 de agosto de 2019 a las 01:15 a.m.** (pág. 7).
  - Resultó vulnerado, además del servidor www.supbienestar.gob.ar, un segundo servidor de la Superintendencia de Bienestar: portal.supbienestar.gob.ar (pág. 7).
  - El atacante obtuvo 1.083 cuentas de correo electrónico con sus contraseñas (pág. 9).
  - Resultaron vulneradas al menos tres (03) terminales informáticas utilizadas por la División Personal Superior (págs. 8 y 9).
  - Se sospecha de una posible infección con software malicioso ("*malware*") en la red de la Policía Federal (págs. 8 y 9).
  - Resultaron filtrados gran cantidad de datos no mencionados por la Policía Federal en el expediente de marras, que excede ampliamente la denuncia del robo de tres (03) cuentas de correo electrónico de Gmail y sus archivos en Google Drive.
  - La Policía Federal nunca descargó la totalidad de los archivos publicados, no pudiendo determinar la magnitud real de la filtración (págs. 9 y 10).

Cabe destacar aquí que el **25 de septiembre de 2019**, solo **tres (03) semanas** después del informe del subcomisario Aguirre y de la respuesta a la DNPDP, la Policía Federal solicitó al juzgado la realización de **seis (06) detenciones y quince (15) allanamientos**, sin incluir ninguna referencia a ninguna investigación interna sobre los servidores de la Superintendencia

de Bienestar ni el resto de las computadoras vulneradas (fs. 537-540). ¿Por qué semejante esfuerzo en supuestamente esclarecer el robo de tres (03) cuentas de Gmail y ninguno en echar luz sobre los graves hechos que la fuerza policial ya conocía de sobra?

SOLICITA

En base a todo lo expuesto y a fines de evitar mayores daños a futuro y poder dilucidar qué es lo que realmente sucedió, solicito a usted tenga a bien:

1. Requerir las declaraciones testimoniales de los subcomisarios **Claudio Ricardo Ramos** y **Carlos Alberto Aguirre**, y del comisario **Ricardo Rubén Rochas** —todos presentes en la declaración de fs. 31-32— a fin de que aclaren qué día la Policía Federal Argentina tomó conocimiento de los correos electrónicos engañosos que aparentaban provenir de la Superintendencia de Bienestar, qué día notaron que servidores de esta dependencia habían sido vulnerados, cuáles fueron estos y qué medidas se tomaron respecto de este hecho y cuándo, qué medidas tomaron para investigar la posible introducción de software malicioso en la red policial y si a la fecha se ha determinado con precisión la cantidad de información que resultó filtrada, la naturaleza y el origen exacto de la misma.
2. Requerir la declaración testimonial del **Subcomisario Diego Hernán Vituzzi** a fin de que aclare qué día tomó conocimiento de las maniobras investigadas en esta causa y cuándo notificó de las mismas a la Superintendencia de Bienestar.
3. Requerir a la Policía Federal aporte la evidencia digital mencionada a fs. 236-243 a los fines de realizar el peritaje correspondiente sobre la misma.
4. Requerir a la División Obtención de Evidencia Digital del Departamento Ciberdelito aporte las imágenes forenses que según la respuesta de la Policía Federal a la DNPDP se tomaron en su oportunidad a los fines de realizar el peritaje correspondiente sobre las mismas.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

Habiendo tomado conocimiento de lo requerido por la Sección INFORMES mediante NO-2019-73436868-APN-SINFO#PFA, el cual guarda relación con lo requerido bajo NO-72377286-APN-DNPDP#AAIP por el Sr. Director Nacional de Protección de Datos Personales de la Agencia de Acceso a la Información Pública, mediante la cual hace referencia al incidente sucedido en la Fuerza consistente en la filtración de información de las Bases de Datos, y conforme las facultades conferidas por la Ley 25.326 y la Decisión Administrativa N° 1002/17, se deberá expedir sobre los siguientes puntos:

1-Indicar desde cuando se tiene conocimiento de la filtración de los datos y que medidas fueron adoptadas en consecuencia.

Respuesta:

Con fecha 12 de agosto del corriente, siendo las 10:40 hs. se toma conocimiento por intermedio de Sr. Director de CIBERCRIMEN del Ministerio de SEGURIDAD DE LA NACION, Lic. Pablo LASARO, que en la plataforma de la red social Twitter y posteriormente Telegram, mediante la cuenta @lagorraleaks, se habían efectuado diversas publicaciones donde los ciberdelincuentes habrían publicado en la red TOR (Deep-Web) 700 Gb de información de esta Policía Federal Argentina.

Ante tal magnitud, se conformó en el ámbito de la Sección CIBERSEGURIDAD un Comité de Crisis, conformado por el Sr. Superintendente FEDERAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES, Director General de INTELIGENCIA CRIMINAL, Director General de OPERACIONES TECNICAS, Jefe del Departamento TECNICO CONTRA EL NARCOTRAFICO, Jefe del Departamento TECNICO OPERATIVO, Jefe A/C del Departamento MOVIMIENTO DE PERSONAL, Director de INVESTIGACIONES CIBERCRIMEN de la Policía de la Provincia de Buenos Aires, Oficiales Jefes de las Distintas Áreas supuestamente alcanzadas.

Posteriormente, y ya teniendo identificado el tipo de información filtrada, la Sección CIBERSEGURIDAD estableció en principio, que unos de los vectores de ataque correspondieron a la intrusión de los ciberdelincuentes a diversas casillas de correos comerciales (Hotmail, Gmail) utilizadas por las dependencias policiales, mediante una técnica de Phishing que fuera detectada, reportada por esta Sección y mitigada con fecha 30/07/2019, por la Sección INFORMATICA de la Superintendencia de BIENESTAR, en razón de que en el sitio de la Página Oficial https://supbienestar.gob.ar se encontraba alojado un formulario malicioso que simulaba ser de un acceso al servicio de Onedrive para la descarga de un archivo, técnica utilizada por el ciberdelincuente para apoderarse de los nombres de usuarios y contraseñas de acceso, según se desprende de las comunicaciones efectuadas por dicha Sección mediante NO-2019-72311832-APN-SINF#PFA y NO-2019-73090818-APN-SINF#PFA.

El Departamento CIBERDELITO, al tomar conocimiento de este tipo de técnica de phishing judicializó la causa en la que interviniera el Juzgado Nacional en lo Criminal de Instrucción N° 6 a cargo de la Dra. María Alejandra PRIVITOLA, Secretaría N° 118 del Dr. Mariano FREIJO.

Asimismo, con fecha 30 de julio del corriente, esta Sección efectuó las comunicaciones de estilo a la Superioridad y se elaboró un Boletín Informativo N° 10, mediante el cual se explicó la maniobra del engaño, se efectuaron las recomendaciones del caso, como ser el cambio urgente de contraseñas para las dependencias que pudieran haber ingresado al sitio malicioso y la obligatoriedad del uso del correo electrónico Institucional para garantizar la veracidad y confidencialidad de la información, entre otras, para conocimiento de la totalidad de las dependencias de esta Institución.

Una vez determinada en forma parcial la metodología de ataque empleada que ocasionara la fuga de información Institucional, se advirtió a la totalidad de las áreas de la POLICIA FEDERAL ARGENTINA, a través de las Divisiones GESTION ADMINISTRATIVA de la amenaza en cuestión, con la finalidad de que la totalidad de las dependencias de cada área proceda en forma urgente al cambio de contraseña de las cuentas de correo electrónico, servicios de almacenamiento en la nube, conexiones WI-FI, y cualquier otro dispositivo que precise credenciales para su acceso. En el mismo sentido, se retransmitió mediante la plataforma del Sistema de Mensajería Electrónica SAFWIN y correo electrónico Institucional, directivas con respecto a cambio de contraseñas de los servicios enunciados anteriormente, como así también en forma indefectible se proceda a la habilitación de un doble factor de autenticación para garantizar un acceso seguro.

En este contexto, el día martes 13 de agosto, se conformaron equipos de trabajo permanentes integrados por profesionales en la materia de ciberseguridad, peritos informáticos, analistas de sistemas y técnicos, entre otros. Dentro de las divisiones de tarea, se crearon grupos de análisis de la información, sanitización de equipos y redes informáticas, detección y alerta temprana de incidentes, y de contacto para evacuar cualquier tipo de consultas relacionadas con seguridad de la información para todas las dependencias policiales, que así l requerían.

Ese mismo día, a partir del análisis de la información obtenida hasta ese momento, y habiendo identificado algunas de las áreas afectadas por la fuga de datos, por disposición de la superioridad, se brindó una charla informativa y de concientización a la Plana Mayor de la institución en el auditorio de la Superintendencia FEDERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, donde se expusieron las técnicas de ataque, las áreas comprometidas, el tipo de información comprometida y el avance de las tareas de análisis que venía desarrollando la Sección CIBERSEGURIDAD.

El día miércoles 14 de agosto, se conformó una reunión del COMITÉ DE SEGURIDAD DE LA INFORMACIÓN, integrada por Oficiales Superiores y Jefes de las principales áreas específicas, donde se expuso entre los presentes los hechos de conocimiento público, a los fines de analizar la cuestión y realizar recomendaciones para mitigar estos sucesos. En esa inteligencia, el Comité elaboro un documento “Normas de Seguridad Informática” con reitero de objetivos inmediatos y a futuro que eviten la fuga de información Institucional.

Con fecha 15 de agosto, el COMITÉ DE SEGURIDAD DE LA INFORMACIÓN convocó a los representantes de todas las áreas de la Policía Federal Argentina, en la que se puso en conocimiento de los de los avances y pormenores del ciberataque, se instrumentó la designación de un oficial de enlace permanente para transmitir o recibir comunicaciones vinculadas a la problemática en cuestión. También se consolidaron los lineamientos de seguridad oportunamente

comunicados, en especial el reitero de la prohibición del uso de cuentas de correo comerciales para el manejo de información institucional.

Ese misma fecha, se enviaron comunicaciones oficiales por el sistema de gestión documental electrónica (GDE), informando a las Divisiones GESTIÓN ADMINISTRATIVA de todas las Superintendencias, a los efectos de advertir mediante listados de Excel embebidos, cuáles eran las dependencias que fueron comprometidas, al mismo tiempo que se reiteraron las medidas de seguridad que deben implementar (backup, escaneos de malware, entre otras) con la finalidad de resguardar toda la información de la dependencia, y, en caso de ser necesario, se proceda a la contención del equipo informático aislándolo de la red e internet.

Posteriormente, con fecha viernes 16 de agosto se convocó a los representantes de cada superintendencia y se los puso en conocimiento de las directivas de buenas prácticas dispuestas por el Comité de SEGURIDAD DE LA INFORMACION en lo relativo a las medidas a implementar en las distintas dependencias de esta Institución.

Con fecha 20 de agosto del corriente año, por disposición del Sr. Superintendente FEDERAL DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES, mediante comunicación a través del sistema de gestión documental electrónica (DGE), NO-2019-74615248-APN-SFTIYCDGA#PFA, comunica las “Normas de Seguridad Informática para su más estricto cumplimiento”, entre las que se reitera el solo uso del correo electrónico Institucional bajo el dominio @policiafederal.gov.ar; la prohibición del almacenamiento de datos en la nube (OneDrive/Google Drive), entre otros.

Con fecha 22 de agosto del corriente, la Sección CIBERSEGURIDAD, tomó conocimiento de un ataque de malware tipo ransomware que involucró equipos informáticos de la Fiscalía de Estado Bonaerense, por lo que se procedió a realizar e informar mediante Boletín Informativo N° 13 a la totalidad de las áreas de la Institución, mediante correo electrónico y a través del Sistema GDE.

El día 23 de agosto, la Dependencia antes mencionada, realiza un informe para concientizar al personal respecto a la amenaza de los ataques de ransomware y la forma de cómo prevenirnos, el cual se distribuye mediante el sistema GDE.

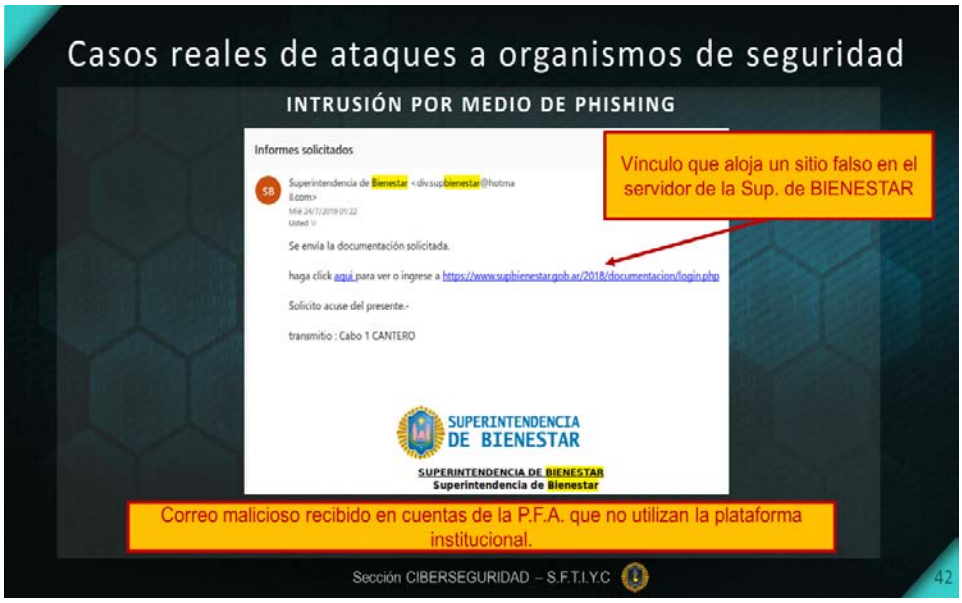
El lunes 26 de agosto del corriente, 18:15 hs. se realiza en el Auditorio de esta Superintendencia, una reunión con los referentes técnicos de las áreas de JEFATURA, SUBJEFATURA, Superintendencias de BIENESTAR, POLICIA CIENTIFICA, PERSONAL INSTRUCCIÓN Y DERECHOS HUMANOS, Direcciones Generales de INTELIGENCIA CRIMINAL, APLICACIONES TECNOLOGICAS, TECNOLOGIAS DE LA INFORMACIÓN, Departamento SISTEMAS CONTRA EL NARCOTRAFICO, Divisiones TECNOLOGIA APLICADA, ANALISIS Y PROSPECTIVA DEL NARCOTRAFICO, CENTRO DE ENTRENAMIENTO TECNOLOGICO, COMPUTACIÓN, TELEPROCESOS, Sección CIBERSEGURIDAD y Personal de la empresa de seguridad informática ESET. La misma se desarrolló en tres etapas:

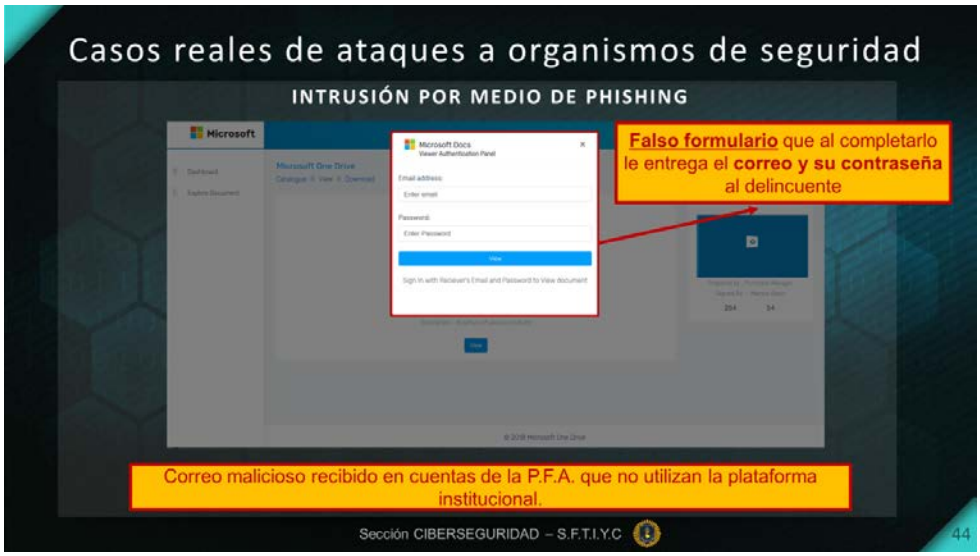
1era Etapa: La Sección CIBERSEGURIDAD interiorizó a los presentes, de la magnitud de los acontecimientos recientes que pusieron en manifiesto las falencias de seguridad informática que se presentaron en las distintas Áreas y Dependencias de esta Policía Federal Argentina, a través de una presentación PowerPoint.

2da Etapa: Personal de la empresa ESET, describió el funcionamiento de sus soluciones que puedan mitigar estos tipos de amenazas y los beneficios que podría traer su implementación en los distintos sectores de esta Institución.

3ra Etapa: Se hizo un cierre de la reunión y se establecieron pautas de trabajo con respecto al desarrollo e implementación de Software, como así también, recomendaciones sobre la estructura de red de las Distintas áreas.

Parte de la presentación disertada por la Sección CIBERSEGURIDAD, puntualizando la metodología de ataque utilizada por los ciberdelincuentes:

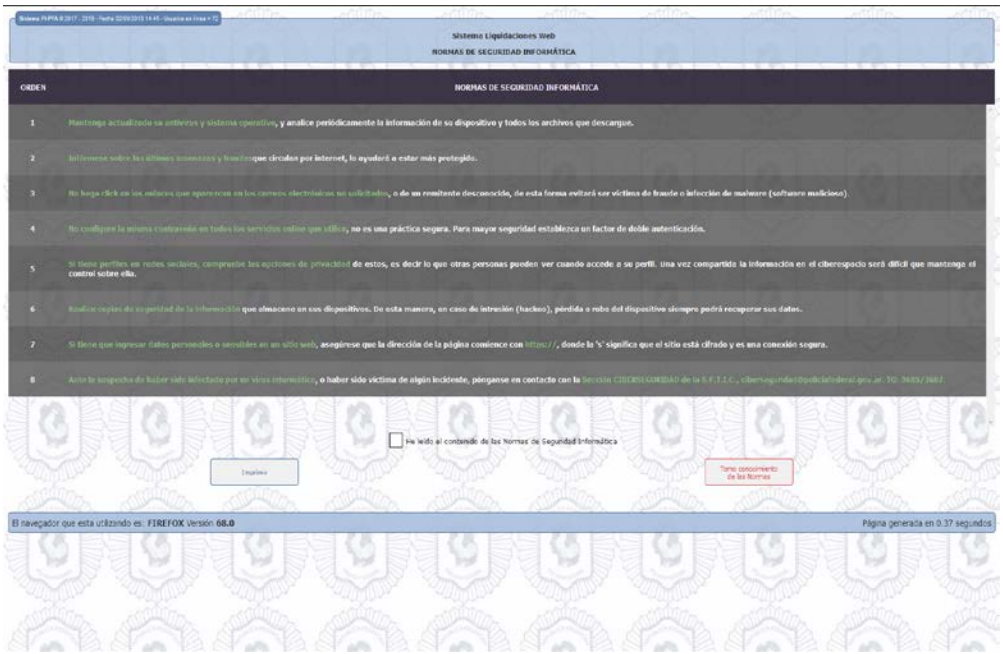


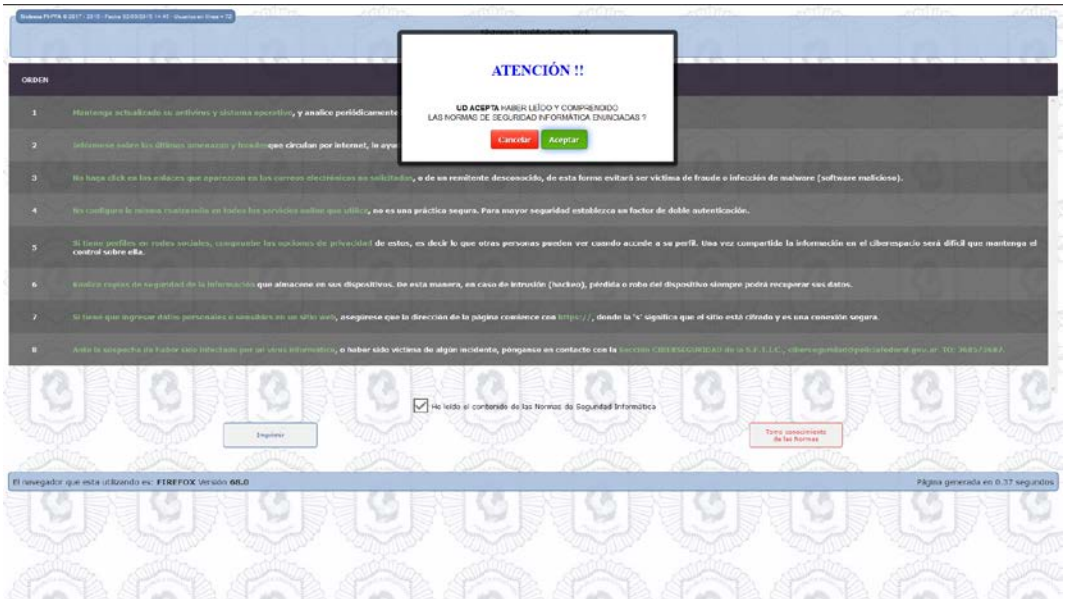


El martes 27 de agosto, la Sección referida, procedió al dictado de una academia alineada con la campaña de concientización que ya se venía realizando durante el año 2018 y 2019 al personal de esta Institución en sus distintos cuadros, Jerarquías y escalafones. Los temas tratados, fueron incluidos como temario obligatorio para la próxima academia que a nivel Institucional se realizan en todas las Dependencias los últimos jueves de cada mes.

En horas de la tarde del mismo 27 de agosto, la División COMPUTACION desarrolló y habilitó a través del Portal PIPFA, una ventana emergente donde se dispone algunas de las Normas de Seguridad Informática, para que de forma obligatoria la totalidad del personal de esta Institución lea y comprenda las mismas. Estas se van a ir modificando en forma periódica y se publicarán con la misma metodología.

Captura de Pantallas Normas de Seguridad Informática





Con respecto a la concientización en temas relacionados con la Seguridad de la Información, durante el año 2018 y 2019 se han dictado diferentes disertaciones, incluso se ha incorporado al Plan Anual de Capacitación DOS (02) Cursos "Introducción a la Seguridad de la Información", siendo realizado uno de ellos en el mes de marzo del corriente y otro en el mes de agosto, al cual han asistido representantes de las distintas fuerzas Federales.

A raíz de lo sucedido se intensificó la cantidad de disertaciones, con el fin de que el personal tome conciencia de los riesgos a lo que se está expuesto con el uso de las Tic´s y las distintas amenazas cibernéticas que cada día se vuelven más complejas con el avance de la tecnología.

Cabe aclarar que, de momento, las implementaciones llevadas a cabo para mitigar este tipo de amenazas fueron realizadas por dependencias técnicas específicas en la materia, no ocasionando erogación alguna para la Institución.

2) Informar cuales fueron las fallas de seguridad que posibilitaron dichas filtraciones

Respuesta:

Para determinar a ciencia cierta cuales fueron las fallas que posibilitaron la fuga de información, se solicitó mediante sistema Gestión Documental Electrónica a las áreas de PERSONAL, DROGAS PELIGROSAS y BIENESTAR a los efectos de que estas amplíen los motivos que dieran origen a la misma, por ser las dependencias propietarias de los datos personales filtrados, mediante NO-2019-75852101-APN-SCIB#PFA.

Cabe aclarar que la información que fuera afectada **NO** corresponde a datos de las bases que concentra los principales servicios informáticos que utiliza esta Policía Federal Argentina, las cuales se encuentran almacenadas en Servidores del Centro de Cómputos de la División

COMPUTACION, sino que pertenecen a datos descentralizados administrados localmente por las áreas anteriormente mencionadas.

Según se desprende de lo informado por la Superintendencia de Bienestar, a través de la Sección INFORMATICA mediante NO-2019-73090818-APN-SINF#PFA que textualmente refiere:

"El día 31 de Julio de corriente año se tomó conocimiento a través de un llamado telefónico del Subcrio VITTUZI, jefe de le Sección Ciberseguridad de la Superintendencia Federal de la Información y las Comunicaciones, de un e-mial enviado de la casilla div.supbienestar@hotmail.com (ajena a esta superintendencia) invitando a los usuarios a ingresar y completar un formulario alojado en nuestra web (www.supbienestar.gob.ar) con el fin de descargar un archivo. El mismo se trataba de un formulario fraudulento que simulaba ser el loguin de One Drive. Inmediatamente se procedió a eliminarlo de nuestra página ya que se comprobó que estaba recopilando correos y contraseñas en forma malintencionada.

El día 12/08 se nos alertó de un "Hacker" que había publicado información personal de los afiliados de esta Policía Federal en la Deep Web.

De inmediato se corroboró de dónde provenía dicha información. Se trata de datos del personal que se obtuvo en formato ".pdf" de los afiliados de la obra social fue realizada mediante un sistema de consulta que fue desarrollado por esta sección (Https://portal.supbienestar.gob.ar/gestion_angel). El mismo se encuentra publicado con el fin de que los anexos del interior puedan consultar el padrón y desempeñar sus funciones en base a esto, solo funciona a modo informativo, es decir, no posee permisos de escritura ni modificación sobre el padrón.

Notamos que la descarga del padrón no se realizó a la fuerza si no que, por el contrario, el ingreso se estableció con usuario y contraseña validos dentro del mismo, las descargas comenzaron el 12 de agosto de 2019 a las 01:15 am en adelante desde la ip de origen 93.188.163.28 que se encuentra asignada al proveedor Hostinger International y a su vez la ip se localizó en la cuidad de Greenville de carolina del sur (E.E.U.U.).

Por otra parte, se habían publicado contraseñas de muchos mails institucionales de esta superintendencia y pudimos concluir que esta información fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmamil. Se estableció que se aprovechó de la información obtenida para poder conseguir acceso a mencionado portal del cual se obtuvo la información publicada.

Según lo informado por la Superintendencia Federal de DROGAS PELIGROSAS, a través del Departamento SISTEMAS CONTRA EL NARCOTRAFICO, donde textualmente reza:

"Respecto a cuales fueron las fallas de seguridad que posibilitaron dichas filtraciones: a) No se cuenta con recursos técnicos y humanos con capacidad para determinar dicha solicitud. b) Se desconocen la totalidad de los datos filtrados, por ende no se puede determinar que se hayan obtenido de esta Superintendencia.

Referente al segundo punto "Detallar que tipo y cantidad de datos personales fueron comprometidos" del Departamento informa, que no se puede determinar tipo y cantidad de datos comprometidos, puesto que no se cuenta con la totalidad de la información compartida en Internet.

No obstante ello, esta Superintendencia viene aplicando políticas de seguridad a fin de evitar esta clase de filtraciones o al menos minimizar la posibilidad que suceda, como ser:

- Cambio de contraseñas cada determinado tiempo

- Cambio de clave de las redes Wifi

- Se promueven diferentes charlas con el personal a fin que tomen conocimiento sobre los peligros de abrir correos no deseados o links que deriven a páginas web desde mails ya sean conocidos o no.

- Se realizan backup periódicos de la información sensible.

Luego del incidente de público conocimiento, se extremaron las medidas de seguridad informáticas como ser:

- Para comunicaciones INSTITUCIONALES se utiliza únicamente el correo de POLICIA FEDERAL bajo el dominio (@policiafederal.gov.ar). Se prohíbe el uso de cualquier otro correo. El correo institucional se encuentra alojado en servidores de esta POLICIA FEDERAL ARGENTINA y se encuentra segurizado mediante una doble validación.

- La información sensible institucional, judicial y de los Recursos Humanos debe estar almacenada en forma SEGURA (encriptada y con contraseña) en las computadoras y/o servidores de las Áreas y Dependencias."

Respecto al área de la Superintendencia de PERSONAL, INSTRUCCIÓN Y DERECHOS HUMANOS, a través de su División PERSONAL SUPERIOR, al día de la fecha no se obtuvo respuesta alguna.

Reunida parte de la información y de acuerdo a las intervenciones del personal técnico de esta Sección, visualizando la información subida por los ciberdelincuentes a la Internet profunda (Deep Web) se puede concluir que las fallas que posibilitaron la filtración de los datos, son atribuidas en un principio al aprovechamiento y explotación de una vulnerabilidad del servidor web administrado por el área de Bienestar lo que ocasionara el alojamiento de un formulario malicioso para ser utilizado mediante la técnica de ingeniería social (Phishing) y obtener las credenciales de acceso a las cuentas de correo no institucionales utilizadas por las dependencias de la esta Policía Federal Argentina y el robo de las fichas en formato ".PDF" de los afiliados a la obra social.

Como segundo factor se debió a una falla humana por parte de los operadores de las cuentas no institucionales que fueran alcanzadas por el correo phishing y que permitió al ciberdelincuente obtener acceso total al servicio de correo tanto de Gmail y Hotmail y la descarga de la información que cada cuenta tenía almacenada en la nube, como ser servicio de OneDrive y Google Drive, que involucrara a Dependencias del área de SUBJEFATURA, Superintendencias Federal de DROGAS PELIGROSAS, PERSONAL, INSTRUCCIÓN Y DERECHOS HUMANOS y AGENCIAS Y DELEGACIONES FEDERALES.

Y como tercer factor de ataque, tras el análisis de esta Sección CIBERSEGURIDAD de los archivos de la Deep Web, se determinó que gran parte de los archivos que se filtraron corresponde a información almacenada en tres terminales informáticas utilizadas por la División PESONAL SUPERIOR, las cuales pudieron haber sido comprometidas por el Ciberdelincuente con una

infección de malware que permitiera el acceso total a los datos allí alojados en los discos rígidos, ya que se corroboró que esta Dependencia no utilizaba el almacenamiento de datos en la nube.

Cabe aclarar que la División OBTENCION DE EVIDENCIA DIGITAL del Departamento CIBERDELITO, realizó imagen forense de los discos afectados y se encuentra en etapa de análisis e investigativa, causa que pasara al fuero Federal e interviniera el Juzgado Nacional en lo Criminal y Correccional Federal N° 9 a cargo del Dr. Luis Osvaldo RODRIGUEZ, Secretaría N° 18 del Dr. Juan Manuel GRANGEAT. Causa N° C-55276/19 Caratulada "N.N S-VIOLACION DE CORRESPONDENCIA"

3) Detallar que tipo y cantidad de datos personales fueron comprometidos

Respuesta:

El área de Bienestar informó: Los datos comprometidos fueron: FICHAS PERSONALES DE LOS AFILIADOS, los cuales contienen los siguientes datos DNI, APELLIDO Y NOMBRE, N° AFILIADO, SEXO, ESTADO CIVIL, FECHA NACIMIENTO, EDAD, TELEFONO FIJO Y MOVIL, EMAIL, DIRECCIÓN, JERARQUIA, SITUACION REVISTA, LEGAJO PERSONAL, DEPENDENCIA, CBU, N° CAJA DE RETIRO, correspondiente a 220 Mil fichas. Asimismo, se divulgaron 1.083 cuentas de correo electrónico bajo el dominio @supbienestar.gob.ar con sus respectivas contraseñas. Los Directorios subidos en la Deep Web se identifican como "INFORMACION PERSONAL, OTRAS BASES DE DATOS".

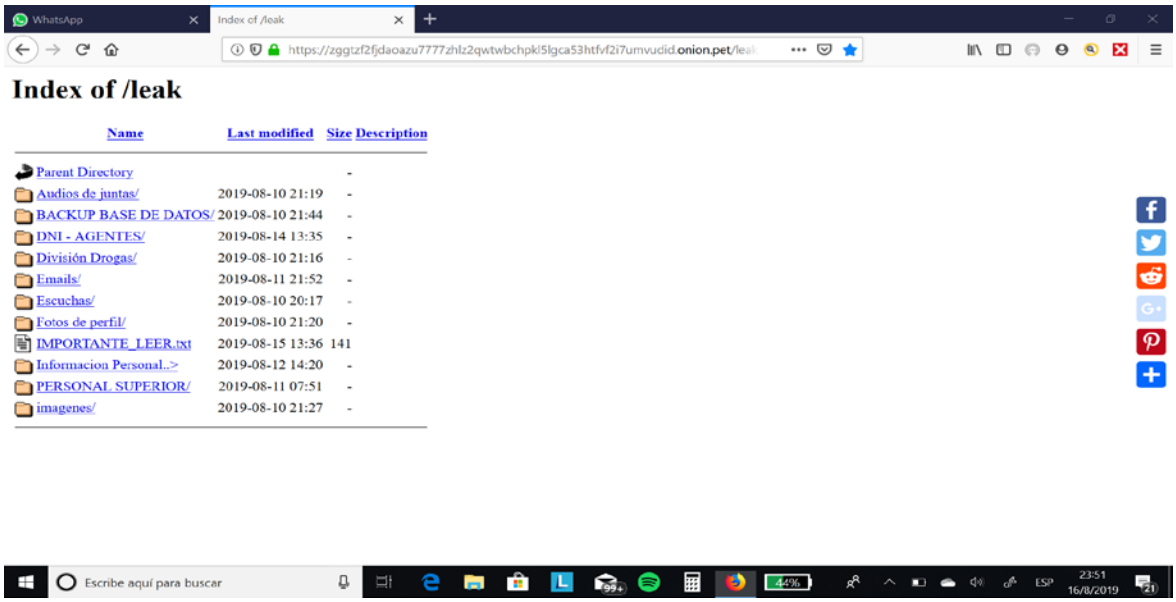
El área de Drogas Peligrosas: Informó que no pudo determinar a la fecha tipo y cantidad de datos personales, por no contar aún con la totalidad de la información compartida en internet.

El área de personal: al día de la fecha no informó tipo y cantidad de datos filtrados.

Hasta el momento esta Sección CIBERSEGURIDAD, no ha podido descargar para su análisis la totalidad de la información filtrada en la Deep Web, debido a que la tasa de transferencia para descarga en muy baja. No obstante, de lo que se desprende de lo visualizado existen gran cantidad de archivos de uso interno y administrativo de distintas dependencias, (.doc, pdf, xls, .rar , jpg, mp4, wav entre otros) que tuviera almacenados en los servicios de almacenamiento en la nube y los propios en discos rígidos internos ya anteriormente explicados.

En relación con información con contenido de datos personales, ampliando lo informado por el área de Bienestar, se observa que, la carpeta identificada en la Deep Web como "DIVISION DROGAS, ESCUCHAS", se hizo un muestreo y se verificó la filtración de 39 fichas con datos y fotos del personal de esa Superintendencia. Respecto a datos con imágenes foto carnet 4x4 de uniforme para uso credencial; DNI escaneados de oficiales en condiciones de ascenso del año 2017; escaneo n° de control credenciales de grado; bases de datos del año 2017 con usuarios y contraseñas sistema "PERSUP"; audios de juntas ascenso, entre otros se encuentran en la carpeta "PERSONAL SUPERIOR, DNI AGENTES, FOTOS DE PERFIL, AUDIO DE JUNTA, BACKUP BASE DE DATOS" del área de personal, hasta el momento no se puede determinar cantidad exacta de los datos filtrados.

A continuación, se procede a adjuntar captura de pantalla de los directorios que se subieron en la Deep Web:



Con respecto a la información filtrada en la Deep Web, desde el día Lunes 02 de septiembre del corriente año, no se encuentra disponible.

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Informe gráfico

Número: IF-2019-80081802-APN-SCIB#PFA

CIUDAD DE BUENOS AIRES
Miércoles 4 de Septiembre de 2019

Referencia: REQUERIMIENTO DIRECTOR AAIP-INCIDENTE-PROTECCION DE DATOS PERSONALES

El documento fue importado por el sistema GEDO con un total de 10 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.09.04 13:54:06 -03'00'

Diego Hernan Vituzzi
Jefe de Sección Subcomisario
Sección Ciberseguridad
Policía Federal Argentina

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.09.04 13:54:07 -03'00'

MANIFIESTA – REITERA – SOLICITA

“La verdad es la verdad, dígala Agamenón o su porquero.
Agamenón: —Conforme.
El porquero: —No me convence.”
(Antonio Machado, “Juan de Mairena”)

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], con el patrocinio de mi abogado defensor Pablo Slonimsqui, en autos caratulados “N.N. Y OTROS S/VIOLACIÓN DE CORRESPONDENCIA, INTIMIDACIÓN PUBLICA Y VIOLACIÓN SIST. INFORMÁTICO. ART. 153 BIS 1° PÁRRAFO. DENUNCIANTE: LA ROCCA, MARIO Y OTROS”, expediente Nº 55276/2019 que tramitan ante el Juzgado Nacional en lo Criminal y Correccional Federal N° 9, Secretaría N° 18, manteniendo el domicilio constituido en el [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V.S. respetuosamente digo:

MANIFIESTA

Que habiendo tomado conocimiento del informe producido por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) firmado por el Dr. Horacio Azzolin (fs. 1681-1692) observamos que sus conclusiones, en lo que respecta a esta parte, reafirman lo ya repetido ad nauseam desde nuestra presentación inicial en el expediente el día (fs. 1157-1161) el 16 de octubre de 2019.

Desde un primer momento reclamamos que V.S. debió haber ponderado los elementos vertidos en los informes policiales que me sindicaban como sospechoso. De tal análisis racional surgiría claro que los supuestos indicios no eran más que un cúmulo de falacias dispuestas con el único objetivo de incriminarme falsamente en los hechos investigados. Se nos respondió, en oportunidad de nuestro planteo de nulidad, que *“nos encontramos en una etapa primaria de la investigación, por lo cual, adentrarse en el estudio tal como pretende el nulidicente, no podrá ser sino por las aristas formales de la diligencia, so pena de adelantar valoraciones propias de otra etapa procesal”*. Con sorpresa encontramos que gran parte del informe de la UFECI se dedica, precisamente, a tal análisis y concluye lo mismo que lo expresado por esta parte. No es esto lo que nos asombra, ya que la verdad es una sola, sino que finalmente —y luego de más de un año y medio de proceso— nos hemos encontrado con alguien normal.

Respecto de la investigación policial dice el fiscal Azzolin:

“En ese sentido, como en toda investigación que se precie de tal, el caso sólo debería construirse a partir de evidencias objetivas que se obtengan de la reconstrucción del hecho. Esto implica recolectar toda la evidencia digital posible y, a partir de ella, recorrer un camino muchas veces difícil, para intentar atribuir el hecho a un individuo o grupo de individuos.

Algunos de esos caminos se recorrieron en la causa y otros parece que se abandonaron sin razón. Además, ***los investigadores habrían tomado ciertos atajos en ese recorrido, efectuando atribuciones en base [a] muchos argumentos genéricos y pocas evidencias concretas; esa senda debería abandonarse****.”*

Dijo esta parte a fs. 1157:

“Puede verse de lo actuado que, ***a la par de una investigación racional****, estructurada sobre elementos objetivos de análisis,* ***mediando una creatividad de dimensiones modestísimas se pretende ubicarme como responsable de algo, de cualquier cosa, vinculado con los hechos investigados, aun cuando surge nítido del legajo mi total ajenidad respecto de los mismos****.*

Y digo así, puesto que habiendo compulsado las actuaciones —por momentos con profundo asombro—, no solo no se advierte que elemento probatorio podría eventualmente sustentar una imputación en mi contra, sino que tampoco se advierte en concreto —ni en abstracto— cuál sería el hecho que se me imputa.”

Más adelante, continúa el fiscal Azzolin:

“Según se desprende de las capturas de fs. 338/539 del legajo de prueba, el grupo administrado por dicho usuario se titulaba "#Lagorra Leaks 2.0", registraba el URL de invitación t.me/LaGorraLeaks, y había sido creado el 16 de agosto de 2019. A fs. 547/548 surge que el usuario poseía asociada la línea [redacted]*. El usuario poseía a su vez otro grupo, registrado también el 16 de agosto, bajo el título "La Gorra leaks Team", cuyo URL resultó ser t.me/LagorraLeaks2. En dicho grupo, su propietario indicó que podían contactarlo por medio del usuario @lagorra (ver fs. 541 y 544/545 del legajo de prueba).*

Se advierte que ambos grupos fueron creados con posterioridad a la desaparición del grupo originario, y si bien el URL del primero coincidiría con el originario, ello podría responder a que aquel fue eliminado, por lo que para el 16 de agosto podía encontrarse ya disponible nuevamente. ***El usuario que se encontraría detrás de estos nuevos grupos (@lagorra) difiere del propietario del grupo primigenio (@gorraleaks).****”*

Dijo esta parte a fs. 1403-1404:

“Este "cambio de canales" ocurrido el 17 de agosto fue notado por varios en la red social Twitter (incluso algunos periodistas me alertaron sobre la mención a mi cuenta), por lo que creí que se trataba de otra maniobra policial tendiente a involucrarme (como puede verse en mis tweets citados en fs. 225 y 231). Ahora viendo el expediente, puedo confirmar mi sospecha: ***los investigadores eran conscientes que se se trataba de dos canales distintos, administrados por personas distintas, pero no lo hicieron notar.”***

Continúa el fiscal Azzolin[1]:

“Cabe señalar que el caso analizado tomó rápidamente estado público, por lo que no sorprende que una gran cantidad de personas relacionadas con dichos sectores [el ámbito de la informática y la ciber-seguridad] hayan mostrado un interés legítimo, emitido diferentes opiniones sobre lo sucedido y publicado información del caso a través de redes sociales. Así, ***las publicaciones y las referencias que pudieran haber efectuado cualquiera de los nombrados sobre el caso y sus conocimientos en la materia tampoco podrían interpretarse como un indicio de su participación en los hechos****.”*

Dijo esta parte a fs. 1180:

“Por último, le hago saber que incluso en mi cuenta de Twitter y en mi blog personal, ambos espacios virtuales que fueron "ciberpatrullados" por las fuerzas de seguridad, actúo como divulgador y comunicador de hechos (en lo referido a mi área de conocimiento), en una tarea también asimilable al periodismo y por ende bajo el paraguas de la libertad de prensa.

De hecho, en esta tarea es que en el año 2017 —presumiendo una grave filtración de datos sensibles de las fuerzas policiales y ante la falta de información en los medios masivos y la falsedad de las declaraciones de funcionarios gubernamentales— fue que me involucré en la investigación de los hechos relacionados con el "hackeo" a la Ministra Bullrich, el Ministerio de Seguridad y la Policía Federal, siendo esto lo que generó la rispidez con esta fuerza y sumó al desagrado de la Ministra Patricia Bullrich hacia mi persona.

Y ahora, en la necesidad de reforzar su autoestima pretenden ubicarme como responsable de algo, echando mano a recursos que la administración de justicia no puede tolerar. Por lo menos en los lugares civilizados.”

Agrega luego el fiscal Azzolin:

1 Todos los resaltados son añadidos por esta parte.

“La situación de Smaldone, si bien similar a la de los anteriores [M. y F.], amerita un mayor desarrollo.

En un informe agregado a fs. 515 y ss., la división policial interviniente elaboró una serie de argumentos tendiente a sustentar la imputación hacia el nombrado.

Por un lado, se intentó validar la hipótesis partiendo del señalamiento realizado por terceros en redes sociales y otras plataformas de internet. Se mencionó también que el nombrado había aludido en ocasiones a diversos ataques informáticos que tuvieron lugar en el país y brindaba información al respecto; que realizó publicaciones en las que cuestionaba el sistema de voto electrónico; que mostraba en sus redes conductas de "hostigamiento" —textual— hacia el personal policial que investigaba causas conexas, como así también aversión a la policía, y que mencionaba en alguno de sus mensajes a usuarios vinculados a aquellas causas.

Desde nuestro punto de vista ***es un conjunto de apreciaciones sin rigor científico ni anclaje concreto en elementos objetivos del caso*** *(las evidencias recolectadas, a las que hicimos referencia anteriormente, parecerían dirigir la investigación hacia otras personas), que pretenden vincular a un perfil determinado de persona con un hecho. O, en realidad, a un posible perfil de persona inferido de las expresiones públicas en una red social concreta que tiene una lógica comunicacional específica; deberíamos tener en claro que los seres humanos somos mucho más que la porción nuestra que se expresa en redes sociales, además de que esa expresión puede no reflejar necesariamente lo que realmente somos y pensamos. En definitiva,* ***las apreciaciones parecen ser propias de otras épocas, colisionan con el derecho a la libertad de expresión y no deberían ser tomadas en cuenta como premisas para construir un caso****.”*

En todo el tiempo transcurrido desde nuestra presentación inicial, esta parte no ha logrado sintetizar tan claramente el dislate de los investigadores policiales, que fuera luego convalidado con el dictado de medidas de vigilancia y seguimiento y, finalmente, de una orden de allanamiento. Realmente, algo propio de otras épocas.

Luego el fiscal Azzolin dedica varios párrafos a analizar uno por uno los elementos que los investigadores policiales esgrimieron como indicios de sospecha y con los que V.S. fundó la orden de mi allanamiento. El resultado es contundente: todos y cada uno de ellos rozan el ridículo. A continuación reproducimos estos párrafos resaltando sus conclusiones:

“Se introdujo además que en los ataques se visualizó información técnica concordante con las descriptas por el actor, tanto en Twitter como en su curriculum vitae. Para empezar, la maniobra involucró el uso de servicios VPN brindados por la firma

DigitalOcean, empresa que Smaldone utilizaría o habría mencionado en sus redes sociales.

Sin embargo, ***cabe destacar que se trata de una empresa con cientos de miles de usuarios****, reconocida mundialmente, con varios años de trayectoria en el mercado, es decir,* ***una empresa cuyos servicios son utilizados potencialmente por gran parte de los profesionales del rubro****.*

Algo similar ocurre con los conocimientos en programación que fueron traídos también a colación, ya que ***los lenguajes PHP, Python y Java se encuentran entre los lenguajes de programación más estudiados y utilizados en la actualidad****.*

En cuanto al servidor NGINX, que Smaldone utilizaría en su sitio web, cabe señalar que ***se trata de un programa informático open source utilizado en alrededor de un tercio de los sitios web activos****.*

En lo que respecta a la coincidente versión del programa utilizada por Smaldone y por los autores de la maniobra (1.16.1), es dable afirmar que ello no respondería necesariamente a una cuestión de preferencia o accesibilidad, sino, probablemente, a que ***se trataba de la última versión estable del programa que se hallaba disponible al momento del hecho****.*

La mención de la compañía de telefonía celular Personal, que sería utilizada por Smaldone, y que coincidiría con la que le brindaba servicio a algunas de las líneas utilizadas para realizar la maniobra, ***carece de cualquier tipo de relevancia en un mercado como el nuestro, en el que el servicio es brindado fundamentalmente por tres empresas.***

A modo de síntesis, ***se trata de supuestas particularidades que, debido a la cantidad, pretenden generar la falsa percepción de que son capaces de reducir el número de sospechosos en un grado tal que permitiría sindicar a un posible responsable. Es una construcción errónea****.*

No caben dudas de que las personas que llevaron a cabo la maniobra tenían conocimientos en la materia.

La dificultad —y, en rigor, el objetivo de la investigación— radica en extraer de la reconstrucción de los hechos evidencias que permitan atribuir el hecho a una persona o grupo de personas. En ese camino, ***si el autor del hecho es sofisticado utilizará varias capas para enmascarar su identidad, entre ellas servicios a nombre de terceros respecto de los cuales un investigador irreflexivo enderezaría la pesquisa****.*

Es por eso que la vinculación de personas al caso por tener determinadas habilidades informáticas (porque todo se reduce a eso) no es suficiente. Un enorme número de individuos responderán a ese perfil y, con ese criterio, deberían también ser investigados. ***Nuevamente son argumentos sin rigor y deberían no tomarse en cuenta.***

Los elementos que se plantean como más objetivos tampoco son suficientes.

En cuanto a la proximidad entre su domicilio ([redacted]* de esta ciudad) y el domicilio consignado al contratar el servicio de FullTech (*[redacted]*) o el domicilio de entrega de los productos adquiridos por algunos de los usuarios de MercadoLibre mencionados anteriormente (*[redacted]*), se advierte que, más allá de las apreciaciones sobre la distancia existente entre los tres domicilios,* ***las tareas llevadas a cabo no permitieron corroborar que Smaldone fuera habido o conocido en sus inmediaciones*** *(ver fs. 544 vta.).*

Se mencionó además que Smaldone había estado cerca del domicilio de la empresa FullTech en fechas próximas a la contratación de sus servicios. Al respecto, debe tenerse en cuenta que los servicios de esta naturaleza suelen contratarse en forma remota, tal como ocurrió en el caso que nos ocupa, por lo que ***se desconoce cuál es la hipótesis a partir de la cual su vinculación con el caso podría verse reforzada a partir de aquella proximidad****.*

Más allá de lo expuesto, a partir del entrecruzamiento realizado con la ayuda del sistema I2 (ver fs. 1534 y ss. del legajo de prueba), se habría establecido que la línea [redacted]*, a nombre de G. C., poseía vínculos con el abonado* [redacted]*, perteneciente a Y. A. G., el cual poseería vínculos con la línea* [redacted]*, que pertenecería a Smaldone. A su vez, este último abonado poseería vínculos con la línea* [redacted]*, que posee un vínculo con la línea* [redacted]*, a nombre de M. M. C., y otro vínculo con la línea* [redacted]*, relacionada con el abonado* [redacted]*, a nombre de J. C. T. y utilizada por tres de los acusados.*

Si bien no se pudieron corroborar desde la Unidad tales extremos —no tuvimos a la vista el material y no correspondería desde un punto de vista metodológico auditar un trabajo ya hecho—, se aprecia que se trata de un elemento probatorio cuyo estudio debería desarrollarse en aras de recabar mayo información sobre las relaciones que sugiere y, de este modo, sobre la eventual vinculación que Smaldone podría poseer con sus consortes de causa.

Desde luego, ***hablar por teléfono no debería, desde nuestro punto de vista, ser el único elemento objetivo para vincular personas que, como sostuvimos a lo largo del presente, las evidencias deberían analizarse a partir de los rastros que dejó el ataque***

informático, o los que los investigadores supieron/pudieron recolectar antes de que se borren*."*

No quisiéramos dejar de aclarar dos cuestiones respecto de los dichos del fiscal Azzolin. La primera, respecto de la supuesta proximidad a las instalaciones de la empresa Full Tech, es que según entendemos la misma se encuentra en la provincia de Entre Ríos, en tanto que los únicos viajes que realizamos por esos tiempos fueron a las ciudades de Santo Tomé y Santa Fe —ambas en la provincia de Santa Fe— en ocasión de la realización de elecciones provinciales y como observador electoral en representación de la ONG Poder Ciudadano, dos días domingo.

La segunda aclaración es —además de negar de plano cualquier relación de esta parte con los nombrados G. C., M. M. C. y J. C. T.— que desconocemos a qué se refieren los investigadores policiales al utilizar la expresión "vínculos" para relacionar dos líneas telefónicas mediante una tercera. Si entendemos por esto que se considera como un indicio una relación de transitividad entre dos números al existir un tercero con el que ambos han mantenido —recibido o realizado— al menos una llamada telefónica, entonces estamos ante un nuevo dislate policial. Piense V.S. solamente en la cantidad de llamadas que se realizan masivamente a través de "call centers", y cómo estas establecerían dicho "vínculo" entre millones de personas. Es vergonzoso que los investigadores, al no encontrar ninguna llamada telefónica de esta parte con ninguno de los demás sospechosos ni con sus familiares, hayan recurrido a este tipo de relación espuria.

Sobre el final, el fiscal Azzolin expone una situación que nos asombra y preocupa:

"Para finalizar, entendemos que la investigación de este caso no debe desatender cierto contexto que fue insinuado y que, por diversas razones, conocemos desde la UFECI.

Los hechos parecerían estar conectados de alguna manera con el ataque que sufriera Patricia Bullrich en 2017 y uno similar que sufriera la actual ministra, Sabina Frederic, al asumir el cargo en 2019.

En este último caso nos tocó intervenir (Legajo UFECI 1646/2019, causa CFP 2905/2020 del Juzgado Federal n° 6) quienes tomaron control de la cuenta publicaron en ella agradeciendo a Smaldone la provisión de las credenciales.

Luego, durante el año 2020, el suscripto recibió mensajes intimidatorios, acompañados de imágenes de abuso sexual infantil, remitidos desde una casilla que pretendía atribuirse al propio Smaldone. En ellas se me amenazaba de muerte por lo actuado en esta causa. El hecho fue denunciado y tramita en la Fiscalía Federal n° 7.

La mención a Smaldone en el ataque a la Ministra Frederic y la burda atribución al nombrado en las amenazas que recibiera quien suscribe cuando ya se nos había dado intervención en el caso no parecen casuales.*"*

Así es que para el titular de la Unidad Fiscal Especializada en Ciberdelincuencia el ataque sufrido por la Ministra de Seguridad Sabina Frederic, la amenaza de muerte recibida por él y hasta la distribución de una imagen de abuso sexual infantil serían nuevos intentos de incriminarme y guardan relación directa con esta causa. Yo mismo he recibido múltiples amenazas de muerte —hacia mí y hacia mis dos hijos, por correo electrónico, Telegram y otros medios— provenientes de personas que decían tener relación con la Policía Federal Argentina, a las que no di entidad en su momento. Pero a la luz de estos hechos, hoy me siento realmente amedrentado y atemorizado. Mientras tanto, al no haberse resuelto mi situación en esta causa, sigo apareciendo públicamente como sospechoso de haber causado un daño a miles de personas (efectivos policiales y sus familias).

REITERA - SOLICITA

En razón de lo expuesto, de V.S. solicito:

- Se expida precisando mi situación procesal.
- Se formule imputación en mi contra y se me tome declaración indagatoria o, en su defecto,
- se dicte mi sobreseimiento en esta causa.
- Se me devuelvan los elementos de trabajo que me fueran secuestrados indebidamente.
- Se ordene la correspondiente extracción de testimonios a los fines de investigar los ilícitos y omisiones cometidos por el personal policial.
- Se investigue lo denunciado por el fiscal Azzolin respecto de la vinculación de la amenaza de muerte recibida y la imagen de abuso sexual infantil intentando incriminarme.
- Se solicite el expediente CFP 2905/2020 al Juzgado Federal n° 6 ad effectum videndi et probandi.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

EPÍLOGO 👋

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], con el patrocinio de mi abogado defensor Pablo Slonimsqui, en autos caratulados "N.N. Y OTROS S/VIOLACIÓN DE CORRESPONDENCIA, INTIMIDACIÓN PUBLICA Y VIOLACIÓN SIST. INFORMÁTICO. ART. 153 BIS 1° PÁRRAFO. DENUNCIANTE: LA ROCCA, MARIO Y OTROS", expediente Nº 55276/2019 que tramitan ante el Juzgado Nacional en lo Criminal y Correccional Federal N° 9, Secretaría N° 18, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V.S. respetuosamente digo:

1 . Sobre mi participación en los hechos

Habiendo presentado a la fecha diez (10) escritos en el expediente de esta causa, considero que ha quedado ampliamente probado mi total ajenidad a los hechos que aquí se investigan, a pesar de no haber tenido hasta ahora ninguna respuesta satisfactoria a mis pedidos. Ha pasado más de un año y medio desde que fui allanado por la policía en el domicilio de mi pareja y luego detenido. Ambos fuimos despojados de nuestras herramientas e información de trabajo —a ella tardaron quince (15) meses en devolvérselas, yo todavía sigo esperando. Mi pareja, mis hijos y yo fuimos vigilados e investigados hasta el abuso por parte de los investigadores policiales, que no pudieron exhibir un solo elemento objetivo que me relacione ni con los hechos ni con los otros supuestos sospechosos. Y como si esto fuera poco, gracias a "fuentes policiales" mi nombre apareció en los medios nacionales bajo la sospecha de ser el organizador de una organización criminal que puso en riesgo al personal de las fuerzas de seguridad y sus familias, con el consiguiente perjuicio personal y laboral, ya que soy un profesional independiente que depende de su imagen pública para ganarse el pan.

2. Sobre el legajo de prueba

Habiendo podido acceder a los primeros ocho (8) cuerpos del legajo de prueba conteniendo parte de la investigación policial, he encontrado mucha más evidencia de las mentiras vertidas y las maniobras realizadas por efectivos de la Policía Federal Argentina tendientes a incriminarme falsamente. Además, encontré nuevos elementos que muestran claramente que he sido objeto de una persecución maliciosa y malintencionada por parte de los investigadores de este caso.

2.1. Falta de investigación inicial

Lo primero que llama la atención es que la investigación policial formalmente se inició el 12 de agosto de 2019 (carátula policial y fs. 01 del legajo de prueba), cuando los hechos investigados fueron denunciados el 30 de julio de 2019 y ocurrieron unos días antes de esta última fecha. ¿Qué hicieron los investigadores durante esas dos semanas? ¿Nada? O, si lo hicieron, ¿por qué no consta en el legajo de prueba? ¿Se decidieron a investigar un hecho que ya al momento de la denuncia era notoriamente grave solo cuando la filtración tomó estado público —coincidentemente— el mismo 12 de agosto de 2019? Este vacío en la investigación es consistente con lo ya expresado y documentado por esta parte en el inciso III del escrito que consta a fs. 1665-1670 respecto de la grave omisión en la denuncia inicial de los hechos ocurridos, esto es, la vulneración de servidores internos de la Policía Federal Argentina, desde los cuales los atacantes obtuvieron el grueso de la información que luego resultara publicada.

Como lo reflejó el periodista Sebastián Davidovsky en el capítulo de su libro que dedica a los hechos investigados en esta causa, citando las palabras de uno de los investigadores policiales: "*Le tocaron el culo al propio jefe, a* Néstor Roncaglia. *No tenemos margen para no hacer nada*"[1]. Todo indica que desde ocurrido el ataque informático hasta hecha pública la filtración eso es exactamente lo que hicieron. Nada.

2.2. Mi introducción en el expediente

El legajo de prueba confirma algo que ya hice notar en el expediente de esta causa. Mi nombre —que hasta ese punto no figuraba directa ni indirectamente en las investigaciones— fue introducido por el **subcomisario Carlos Alberto Aguirre** en su informe del 15 de agosto de 2019 (fs. 159-160 del legajo de prueba), cuando dijo que:

> *"Ante esta situación habiéndose comprobado la autoría de los autores involucrados en el hecho del hackeo a la cuenta de Twitter de la Ministra en el año 2.017, y la capacidad técnica que estos presentan para llevar a cabo los presentes hechos, y habiendo encontrando publicaciones donde se adjudican estos al mismo tiempo, se considera a estos como posibles responsables del hecho tratandose de las siguientes personas: R.D.M.M […] E.V.C [...] JAVIER SMALDONE [...]*
>
> *Por último y en base a la investigación de las maniobras efectuadas en el año 2.017, se pudo observar mediante fuentes abiertas publicaciones de autos de procesamiento referidos a la causa del hackeo a la cuenta de Twitter de la Ministra de Seguridad, donde se hace referencia a un tercer involucrado en dicha maniobra bajo el usuario @Capitan_Alfa, usuario bajo el nombre de AEF"*

1 Sebastián Davidovsky. "Engaños Digitales, Víctimas Reales". Ediciones B, 2020. Página 30.

La realidad es que no hay ninguna publicación en la que yo me adjudique ningún tipo de participación en los hechos investigados —solo tweets poniendo de manifiesto la gravedad de lo ocurrido. Y con respecto a la causa por el hackeo a la por entonces ministra Patricia Bullrich (CFP 1033/2017, Juzgado Nacional en lo Criminal y Correccional Federal Nº 2), la misma aún no ha sido juzgada y tiene como únicos procesados a los mencionados M.M y V.C.

De hecho, en el auto de procesamiento en el que el subcomisario Aguirre dice haberse basado puede leerse claramente que nunca hubo una imputación hacia mi persona[2]. Y no solo eso, sino que en dicha causa aporté prueba y me fue tomada declaración testimonial, como puede verse en la copia aportada por mí a fs. 1162-1164 en el expediente de marras.

Recordemos que dos días antes de presentado el informe del subcomisario Aguirre, el 13 de agosto de 2019, prestó declaración en sede judicial el **subcomisario Claudio Ricardo Ramos** (fs. 31-32 del expediente), en presencia del propio Aguirre, y solo mencionó como sospechosos a M.M y a V.C.

¿Qué más debo hacer para demostrar que el **subcomisario Carlos Alberto Aguirre** a sabiendas me incriminó falsamente, inventando no solo mi participación sino además mi culpabilidad en los hechos acaecidos en 2017? Si hasta cometió un error revelador al introducir un cuarto sospechoso llamándolo *"tercer involucrado"*, redacción seguramente anterior al añadido de mi nombre a la lista.

2.3. Las cámaras secretas de vigilancia

A fs. 433 vta. del expediente se dice que el personal policial instaló cámaras de vigilancia frente a mi domicilio en la ciudad de Río Cuarto, donde viven mis hijos. A fs. 1063 del legajo de prueba puede verse una orden firmada por el subcomisario Aguirre donde *"se solicita implantar un sistema de Video-Vigilancia encubierto sobre el domicilio de la calle* [redacted] *N.º 1236, de la Ciudad Autónoma de Buenos Aires"*, lugar donde los investigadores policiales vieron ingresar a alguien que creyeron se trataba de mí, luego de deambular varios días por las calles en un área de ocho manzanas. Sí, me confundieron con otra persona y pusieron una cámara oculta frente a su domicilio.

¿Cuál era el interés de quienes investigaban un delito informático ocurrido meses antes de tener filmaciones de la puerta de mi vivienda? ¿Qué urgencia los llevó a poner una cámara frente al edificio de alguien que ni siquiera se molestaron en verificar que realmente fuera yo? Aún luego de revisar ocho (8) cuerpos del legajo de prueba, no puedo encontrar cuál es la hipótesis policial sobre mi participación en los hechos.

2 https://www.cij.gov.ar/nota-25080-El-juez-Ramos-proces--a-un-imputado-por-el--hackeo--a-la-cuenta-de-Twitter-de-la-ministra-Patricia-Bullrich.html

2.4. Solicitud de datos a Whatsapp

Una de las medidas que se tomó conmigo —y no con otros de los investigados— fue la solicitud de todos los datos de la cuenta asociada a mi número telefónico en el sistema WhatsApp (fs. 1319 del legajo de prueba). Sin embargo en el mismo legajo pueden verse una gran cantidad de mensajes de este sistema, así como también referencias a cuentas de otros números telefónicos, producto de peritajes y otras medidas de prueba (ver por ejemplo, fs. 233 vta., 241, 312, 858 vta., 1412 vta., 1427, 1438, 1462 a 1468).

¿Por qué no se pidió a WhatsApp información sobre estos números? ¿Por qué se pidió sobre el mío, aún cuando en todo lo actuado no aparece ni una sola mención a un mensaje de WhatsApp enviado o recibido por mí? Tal parece que a los investigadores policiales solo les interesaba la información de mi cuenta y la de nadie más. Una nueva muestra de la arbitrariedad con que se condujeron.

2.5. Solicitud de datos de la tarjeta SUBE

Otra medida dispuesta solo respecto de esta parte —y de ningún otro investigado— fue la obtención de información sobre el uso de la tarjeta de transporte público SUBE, mediante la cual se intentó averiguar mis desplazamientos en la ciudad de Buenos Aires. Aquí los investigadores policiales, además, hicieron aparecer (a fs. 1302 del legajo de prueba) el nombre completo y el número de documento de mi pareja.

¿De dónde lo obtuvieron? ¿Por qué no figura antes en ningún lugar del legajo de prueba? ¿Mediante qué medida de vigilancia lograron determinar con precisión mi relación con ella y sus datos personales?

2.6. Las redes Wi-Fi como indicio

En el informe policial incluido a fs. 433 vta. (que no se encuentra en la parte del legajo de prueba al que tuve acceso) se dice que, aludiendo a mi domicilio en Río Cuarto, que *“una de las señales de Wi Fi próximas al domicilio investigado, podrían vincularse con el símbolo de los atacantes [S]”*. Aún entendiendo que para alguien ignorante de informática esto pudiera representar algún grado de sospecha, la realidad es que cuando examinamos las fs. 681 y 682 del legajo de prueba encontramos las siguientes fotografías, que supuestamente muestran las redes Wi-Fi próximas a mi vivienda:

¿Cuáles de estos nombres *"podría vincularse con el símbolo [S]"* y de qué manera? Ni más ni menos, otra tomadura de pelo de los investigadores policiales tendiente a engañar a V.S. haciéndome parecer sospechoso. (Un detalle adicional: mi red Wi-Fi tenía como nombre por aquel entonces "tuxland", que no aparece en las capturas policiales).

2.7. Los supuestos vínculos telefónicos

Con respecto a los supuestos vínculos entre mi número de teléfono y el de otros investigados, mencionados a fs. 1534 vta. del legajo de prueba, como ya dije en mi escrito del día 23 de abril de 2021, los investigadores policiales nunca precisan qué entienden por "vínculo". Sospecho fuertemente que se trata de una relación espuria, intentando vincular dos números telefónicos transitivamente a través de un tercero con el cual han establecido —recibido o realizado— llamadas. Como bien afirmó el fiscal Horacio Azzolin al analizar este punto: "*hablar por teléfono no debería, desde nuestro punto de vista, ser el único elemento objetivo para vincular personas"*. Mucho menos debería serlo el tener un número de contacto en común que bien podría ser el de un call center o de un prestador de servicios.

En el informe policial que consta a fs. 1534-1535 del legajo de prueba se dice que el personal policial *"hace entrega a la instrucción del resultado obtenido, el cual se guardó en UN (1) CD, para poder observar con mayor claridad y realizar el correspondiente análisis por parte del personal abocado a la pesquisa"*. Además, en dicho informe se menciona la existencia de tres (3) diagramas y otros tres (3) informes sobre los entrecruzamientos telefónicos realizados, ninguno de los cuales está incluido en la porción del legajo de prueba a la que tuve acceso. No contando con dichos elementos no puedo determinar precisamente qué tipo de vinculación con otros autores de la causa intentaron falazmente sugerir.

2.8. Mi interés por el sistema electoral

A fs. 215 vta. del legajo de prueba encuentro algo realmente alarmante e inadmisible. Dicen los investigadores policiales:

“En el caso de @Mis2centavos, es un usuario con gran actividad en la Red social TWITTER, quien mayormente muestra su descontento con el gobierno actual, el sistema de recuento de votos y realiza algunos comentarios referentes al hackeo de #Lagorraleaks.

Con lo que respecta puntualmente en el dia de ayer a la noche, realiza un comentario alrededor de las 19:49 pm objantando que por una hora estara ocupado realizando un nota en su blog (la cual posteriormente finalmente la subio). Cabe mencionar, que paralelamente a esto, horas antes en el grupo de Telegram el administrador manifestaba que se encontraba organizando el ataque masivo.”

Luego, a fs 216 del legajo de prueba, adjuntan una captura del siguiente tweet:

Haciendo caso omiso a las múltiples ofensas al idioma español, es realmente grave que para los efectivos de la Policía Federal Argentina sea motivo de sospecha que un ciudadano muestre su descontento con el gobierno y que dedique parte de su tiempo a preocuparse y ocuparse del sistema electoral, pilar del sistema democrático. ¿Resulta de algún modo sospechoso que yo estuviera escribiendo —de *motu proprio*, sin remuneración ni recompensa alguna— un artículo sobre las elecciones nacionales que acababan de realizarse, a la vez que alguien por ahí anduviera amenazando con atacar a la policía? ¿O es, más bien, todo lo contrario? ¿No me muestra eso —además de como un ciudadano comprometido— como alguien que estaba ocupado en cosas más importantes que asustar a la Policía Federal Argentina? La realidad es que incluir esto como un indicio en mi contra, de lo único que habla es de la actitud poco democrática de ciertos elementos dentro de esa fuerza y de su animosidad contra mí.

En honor a la brevedad, omitiré referirme aquí a los dislates del informe policial que consta a fs. 515-532 del expediente (pero que desafortunadamente no aparece en la parte del legajo de prueba al que se me dio acceso). Además, los argumentos falaces esgrimidos por los investigadores en esa pieza vergonzosa ya fueron expuestos como tales en el informe presentado a fs. 1681-1692 por la Unidad Fiscal Especializada en Ciberdelincuencia. Pero habiendo repasado (parte de) la investigación policial en detalle, no puedo dejar de recordar las palabras allí vertidas por el fiscal Horacio Azzolin respecto de las maniobras de la Policía Federal Argentina tendientes a incriminarme: “*parecen ser propias de otras épocas”*. La referencia al tweet y a mi artículo sobre las elecciones refuerza esa apreciación.

2.9. El resto del legajo de prueba

Es notable —y angustiante, y preocupante— ver que allá por el 24 de septiembre de 2019, cuando el expediente judicial aún no completaba su tercer cuerpo, el legajo de prueba con la investigación policial ya sumaba ocho (8) cuerpos terminados. Y me inquieta de sobremanera con qué podría encontrarme de tener acceso al resto. Aunque —y seguiré insistiendo en esto— tengo la certeza de que no hallaría algo que realmente justifique una sospecha fundada para proceder al allanamiento que fue ordenado el día 3 de octubre de 2019.

3. La confesión de la Policía Federal Argentina

3.1 El reconocimiento de un hecho anterior

El legajo de prueba contiene un elemento novedoso y asombroso, que al parecer no fue notado ni por los instructores de esta causa ni por la Unidad Fiscal Especializada en Ciberdelincuencia. A fs. 591-592 del mismo consta una nota enviada por personal de la Superintendencia de Bienestar de la Policía Federal Argentina a los efectivos policiales Diego Hernán Vituzzi, Gonzalo Fabián Danier y Claudio Ricardo Ramos el **21 de agosto de 2019**, donde se lee:

> *"Se pone en conocimiento sobre los hechos de público conocimiento acerca de la reciente publicación de tres bases de datos de esta Superintendencia publicadas con fecha 19 de Agosto del corriente año (Captura de la publicación embebida). Las mismas se encontraban alojadas en el servidor web que fue vulnerado en la ocasión anterior. Ni bien tuvimos conocimiento del primer hurto de información tomamos la acción inmediata de sacar de internet todos nuestros servicios con el fin de evaluar vulnerabilidades evitando que continúen en él. Estas tres bases de datos son aplicaciones menores del servidor que ya se encontraban en su poder y decidió publicarlas un tiempo después.*
>
> > *MYSQL 170717 .SQL: Esta base de datos se utilizó para realizar encuestas en el año 2017.*
> >
> > *PFA WEB Bienestar .SQL: Esta base de datos también data del año 2017 [...]"*

La policía reconoce aquí que algunas de las bases de datos filtradas y luego publicadas "*se encontraban alojadas en el servidor web que fue vulnerado en la ocasión anterior*". ¿Cuál fue ***"la ocasión anterior"*** en que se vulneró un servidor web de la Superintendencia de Bienestar, el ***"primer hurto"***? Tal parece que fue allá por el año 2017. ¿Hubo alguna denuncia judicial al respecto? Por lo pronto, no se hizo referencia alguna a este hecho precedente en ningún lugar

del expediente de marras (apenas esta nota perdida en medio de un extensísimo “legajo de prueba”).

3.2 La advertencia de 2017

Recordemos que a comienzos de 2017 ocurrió primero un “hackeo” de la cuentas de Twitter y de correo electrónico oficial de la por entonces Ministra de Seguridad Patricia Bullrich y luego la vulneración de cuentas oficiales de la Policía Federal Argentina. En dicha oportunidad, además de prestar declaración testimonial en la causa CFP 1033/2017 (ver fs. 1162-1164), presenté prueba sobre este último punto.

En el adjunto del escrito presentado por la defensa de V.C. el día 8 de abril de 2021 puede verse una orden emitida el 9 de mayo de 2017 por el juez instructor de la causa CFP 1033/2017, dirigida al por entonces Jefe de la Policía Federal Argentina, Comisario General Néstor Ramón Roncaglia, instruyéndole “*que, con caracter de muy urgente, se adopten las máximas medidas de seguridad posibles para resguardar la información sensible contenida en sistemas y/o servidores electrónicos de esa policía federal”*.

En el informe policial IF-2019-80081802-APN-SCIB#PFA del 4 de septiembre de 2019, que consta a fs. 1702-1707, la Superintendencia de Bienestar reconocía respecto de la información filtrada *“pudimos concluir que esta información fue obtenida mediante la inyección de código PHP que tuvo lugar en una vulnerabilidad del PHP 5.6.3 de panel webmail”*. La conclusión inevitable —como ya expliqué y documenté a fs. 1677-1678— es que a la fecha de ocurridos los hechos investigados (julio de 2019), el servidor web de la Superintendencia de Bienestar utilizaba software vulnerable que databa de noviembre de 2014. No adoptaron las máximas medidas de seguridad, ni tampoco las mínimas. La Policía Federal Argentina desoyó hasta la orden de un juez federal respecto de actualizar sus servidores.

3.3 El ocultamiento y la persecución

El 30 de julio de 2019, al presentar la denuncia judicial por el ataque sufrido, la Policía Federal no dijo lo que era evidente ya en ese momento y de ninguna manera podían desconocer: que servidores de la Superintendencia de Bienestar habían sido vulnerados y los atacantes habían extraído cuantiosa información de ellos. No podían decirlo, porque no lo dijeron cuando ocurrió en el año 2017 y porque tampoco escucharon la voz de alerta de la Justicia Federal.

¿Y qué hizo luego la Policía Federal Argentina? Nada. Por espacio de dos semanas, como muestran claramente tanto el expediente como el legajo de prueba, no se investigó. Hasta que el 12 de agosto de 2019 los datos previamente filtrados —incluso algunos del ataque de 2017— fueron publicados en Internet. ¿Y cuál fue la primera medida que tomaron entonces? Intentar inculpar a quien desde hacía más de dos años alertaba sobre el estado de abandono de sus

servidores y el encubrimiento de los ataques y las filtraciones ocurridas. Esto es lo que dije en la red social Twitter a pocas horas de conocerse públicamente la filtración (algo que la policía nunca incluyó en sus extensos informes ocupándose de mis tweets)[3]:

Acto seguido, el 15 de agosto de 2019 en el informe de fs. 67-68 el subcomisario Carlos Alberto Aguirre me sindicó como sospechoso de este nuevo ataque, llegando al extremo de inventar que yo había sido el autor del ocurrido en el año 2017. Y luego siguió la consabida farsa de investigación policial, que en base a mentiras, conjeturas descabelladas, asociaciones ridículas y alusiones a mis opiniones políticas pretendieron justificar mi allanamiento, detención —lamentablemente, con todo éxito— y una imputación que a más de un año y medio todavía no ha podido ser formulada. Todo con el único objetivo de amedrentarme. La conocida estrategia de matar al mensajero, sobre la que se explayó debidamente el fiscal Horacio Azzolin en el informe de la UFECI de fs. 1681-1692, donde además denunció haber recibido amenazas de muerte e imágenes de abuso sexual infantil como parte del intento de incriminarme.

4. Para finalizar

No habiendo ningún elemento objetivo que me vincule de forma alguna con los hechos investigados en esta causa, ni siquiera con alguno de los demás investigados, es inadmisible que aún me encuentre en este expediente y que se continúe privándome de mis herramientas de trabajo y mis datos, prolongando además la afectación de mi buen nombre y honor.

A mi entender la filtración de datos de la Policía Federal Argentina —la mayor de la que se tenga noticia en nuestro país a la fecha— constituye un hecho gravísimo, pero también lo es el ocultamiento realizado por efectivos de esta fuerza de forma continuada desde los sucesos del año 2017. Y esto resulta agravado por las técnicas utilizadas por la policía para, además, intentar incriminar a alguien que desde el primer momento alerta públicamente sobre las posibles consecuencias de la inacción y el encubrimiento. Todo esto con maniobras que —y uso nuevamente las palabras del titular de la UFECI— *"parecen ser propias de otras épocas"*.

Tener presente lo expuesto, SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

3 https://twitter.com/mis2centavos/status/1161057262321983488

MANIFIESTA – SOLICITA

> *“No hay ningún error. El organismo para el que trabajamos, por lo que conozco de él, y solo conozco los rangos más inferiores, no se dedica a buscar la culpa en la población, sino que, como está establecido en la ley, se ve atraído por la culpa y nos envía a nosotros, los vigilantes. Eso es ley. ¿Dónde puede cometerse aquí un error?”*
>
> *(Franz Kafka, “El Proceso”)*

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI N.º [redacted], con el patrocinio de mi abogado defensor Pablo Slonimsqui, en autos caratulados “N.N. Y OTROS S/VIOLACIÓN DE CORRESPONDENCIA, INTIMIDACIÓN PUBLICA Y VIOLACIÓN SIST. INFORMÁTICO. ART. 153 BIS 1° PÁRRAFO. DENUNCIANTE: LA ROCCA, MARIO Y OTROS”, expediente Nº 55276/2019 que tramitan ante el Juzgado Nacional en lo Criminal y Correccional Federal N° 9, Secretaría N° 18, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V.S. respetuosamente digo:

MANIFIESTA

I

Habiendo visto el expediente 534/2019 de la Procuraduría de Investigaciones Administrativas (PIA), observo que en el análisis realizado en las fs. 67 a 85, firmado por el Jefe de Despacho Manuel Riveiro Gionis, se destacan varias de las observaciones que ya fueron hechas por esta parte. En particular, las referidas a las discrepancias entre lo denunciado por efectivos de la Policía Federal Argentina en un primer momento (30 de julio de 2019) y luego de tomar estado público la filtración de datos confidenciales (12 de agosto de 2019), como así también las deficientes medidas de seguridad tomadas para preservar dichos datos incluso después de acaecidos los hechos que motivaron la presente causa penal.

A fs. 58 de dicho expediente se incluye un pedido de la PIA a la Ministra de Seguridad Lic. Sabina Frederic, de fecha 29 de octubre de 2020, en el que se requiere la remisión de copias del sumario administrativo n.º 465-18-001.840/19 caratulado “ESCLARECIMIENTO DEL HECHO Y DE CORRESPONDER JUZGAR LA CONDUCTA DE SUS RESPONSABLES” del Departamento de Investigaciones Administrativas de la Superintendencia de Asuntos Internos e Inspección General de la PFA. Dicha solicitud fue respondida a fs. 62 por nota NO-

2020-86912330-APN-DNCJYMP$MSG, de fecha 14 de diciembre de 2020, en la que se dice que *"se adjunta un link de google drive para su acceso debido a que el archivo es muy pesado para enviarlo adjunto por correo electrónico"*, seguido del siguiente enlace:

https://drive.google.com/file/d/10TAfMte_QH-[redacted]/view?usp=sharing

Dicho enlace —que al menos hasta el 11 de junio de 2021 podía ser accedido de forma irrestricta— permitía descargar el mencionado sumario administrativo de la Policía Federal Argentina, que había sido solicitado a V.S. por esta parte ad effectum videndi et probandi a fs. 1669.

Entre varias cuestiones en las que por el momento no ahondaré, me llama la atención que en este sumario de Asuntos Internos aparezca incluido el contenido completo de cinco (05) notas periodísticas en las que aparezco mencionado o entrevistado, todas ellas posteriores al allanamiento de mi domicilio y mi detención, en lo que la policía describe como *"exploración de prensa"*. Incluso una de ellas fue escrita por mí, publicada en mi blog personal y reproducida íntegramente por un medio periodístico. Nunca hubiera imaginado —bueno, en los últimos tiempos sí— que las investigaciones internas de la Policía Federal Argentina consistían en analizar qué se dice de ellos en los medios de comunicación. Ochenta y tres (83) fojas del total de cuatrocientas cuarenta y cinco (445) del sumario en cuestión corresponden a tales "exploraciones de prensa". Nuevamente hago mías las palabras del fiscal especializado en ciberdelincuencia Horacio Azzolín en su informe presentado en esta causa a fs. 1689: estas prácticas también *"parecen ser propias de otras épocas"*.

II

He observado que la única medida de prueba propuesta por el fiscal Horacio Azzolín en su dictamen de fs. 1681-1692 a la que se le ha dado curso es al envío de un exhorto a las autoridades de los Estados Unidos, requiriendo información sobre cuentas de Twitter y direcciones IP. Teniendo en cuenta que los hechos investigados ocurrieron entre el 24 y el 30 de julio de 2019, y entendiendo que la legislación estadounidense no obliga a los proveedores de comunicaciones y servicios de Internet a mantener tales registros más allá de los dieciocho (18) meses, es de suponerse que dicha medida —que debió tomarse de inmediato y que hasta hace pocos días todavía presentaba dificultades a la fiscalía interviniente— difícilmente pueda arrojar algún dato esclarecedor. Sin perjuicio de lo expuesto, habré de solicitar se indague sobre el estado de este trámite.

SOLICITA

Por lo expresado, solicito a V.S.:

- Se incorpore a este expediente el sumario 465-18-001.840/19 de la Policía Federal Argentina, por considerarlo necesario para ejercer mi derecho de defensa.

- Se tenga presente la inclusión de notas periodísticas referidas a mi persona en dicho sumario como otro elemento probatorio de la persecución infundada, el ensañamiento y la arbitrariedad de los investigadores policiales.

- Se consulte, a través de la vía pertinente, sobre el estado del exhorto enviado a la Justicia de los Estados Unidos.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

MANIFIESTA – REITERA – SOLICITA

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI N.º [redacted], conjuntamente con mi abogado defensor Pablo Slonimsqui, en la causa Nº 55.276/2019 caratulada *"NN S/VIOLACIÓN DE CORRESPONDENCIA"*, que tramita en la Secretaría n° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V. S. me presento y digo:

MANIFIESTA

El **08 de agosto de 2021** se acaban de cumplir **veintidós (22) meses** de que allanaran mi domicilio y secuestraran mis herramientas, llevándose con ellas información sensible e indispensable para mi trabajo. Durante todo este tiempo no hicieron nada, más que dejarlas volverse obsoletas y ocasionarme un perjuicio. Y no parece haber, a juzgar por los movimientos en el expediente, ninguna intención de realizar alguna forma de peritaje sobre su contenido en un futuro cercano. Los oficiales de la Policía Federal que me incriminaron falsamente se salieron con la suya, el daño ya está hecho. **Habida cuenta de ello, habré de solicitar su inmediata devolución.**

Desde un primer momento dije a V.S. que la investigación policial en la que se basó la orden de allanamiento era un auténtico mamarracho –no solo informático sino también jurídico–, partiendo de una afirmación comprobable y comprobadamente falsa del subcomisario Carlos Alberto Aguirre (fs. 68). Aunque se me negó tener razón, tuvo que venir un fiscal especializado en delitos informáticos, el Dr. Horacio Azzolin, **un año y medio después** a desglosar punto por punto cada uno de los dislates policiales tendientes a hacerme aparecer como sospechoso (fs. 1681-1692). Ni más ni menos, lo mismo que había hecho yo en mi primera presentación (fs. 1157-1161), y que complementé con otras que ya no me alcanzan los dedos de las manos para contar. Dijo el fiscal Azzolin que *"los investigadores habrían tomado ciertos atajos […], efectuando atribuciones en base [a] muchos argumentos genéricos y pocas evidencias concretas"* (fs. 1682 vta.). Y definió al intento –lamentablemente exitoso– de involucrarme como *"un conjunto de apreciaciones sin rigor científico ni anclaje concreto en elementos objetivos del caso (las evidencias recolectadas, a las que hicimos referencia anteriormente, parecerían dirigir la investigación hacia otras personas), que pretenden vincular a un perfil determinado de persona con un hecho"* (fs. 1689), concluyendo además que *"**las apreciaciones parecen ser propias de otras épocas**, colisionan con el derecho a la libertad de expresión y no deberían ser tomadas en cuenta como premisas para construir un caso"* (fs. 1689). Sí, el titular de la UFECI comparó la investigación realizada por la Policía Federal Argentina con los métodos de las dictaduras militares. Y como si esto fuera poco, también dijo haber recibido

amenazas e imágenes de abuso sexual infantil como un nuevo intento de incriminarme (fs. 1692). Más claro, agua.

Pero ahora veo que, **desde hace casi cuatro meses**, andan dando palos de ciego para escribir un exhorto que debería haber sido enviado a la Justicia de los EE. UU. a pocos días de ocurrido el hecho, y que seguramente no tendrá ningún resultado positivo, ya que se pide información anterior al 7 de agosto de 2019, **hace más de dos años**. Parece que entre un Juzgado Federal Criminal y Correccional y una Fiscalía Federal Criminal y Correccional, pidiendo ayuda a una Unidad Fiscal Especializada en Ciberdelincuencia y hasta a la Policía de la Ciudad de Buenos Aires, tienen terribles problemas para determinar cuál es la hora oficial de la Argentina (Ley 26.350). Hasta el Instituto Geográfico Nacional no paramos.

Mientras tanto, como ya mostré en este expediente (fs. 1665 vta.), mi nombre aparece en los principales medios de prensa de la Argentina –siempre a instancias de "fuentes policiales"– como sospechoso de haber publicado información que puso en riesgo la vida de muchas personas. Por esta situación aún hoy sigo recibiendo insultos y amenazas, no solo a través de las redes sociales, sino por medios directos de contacto como correo electrónico, WhatsApp y Telegram. Nuevamente le recuerdo que, a diferencia de usted, debo ganarme el pan consiguiendo clientes mes a mes, y para ello dependo de mi buena reputación.

Lo que no logro dilucidar, y solo tengo penosas opciones por las que decantarme, es si el Ministerio Público es partícipe de la maniobra policial tendiente a involucrarme, si se trata solo de un rasgo distintivo de su personal el no atender razones, o si enfrento una estructura burocrática que se ha hecho un nudo con su propia incompetencia.

REITERA - SOLICITA

En razón de lo expuesto, de V.S. solicito:

1. Se me devuelvan mis herramientas con mis datos, toda vez que el trámite de lo actuado exhibe sin matices la ausencia de razones que justifiquen su secuestro.
2. Se me desvincule de esta causa, cesando en la afectación de mi buen nombre y honor.
3. Se investiguen los ilícitos y omisiones cometidos por el personal de la Policía Federal Argentina en esta causa.
4. Se investigue lo denunciado por el fiscal Horacio Azzolin respecto de la vinculación con esta causa de la amenaza de muerte recibida y la imagen de abuso sexual infantil intentando incriminarme.

Proveer de conformidad será una muestra de racionalidad y SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

MANIFIESTA – SOLICITA

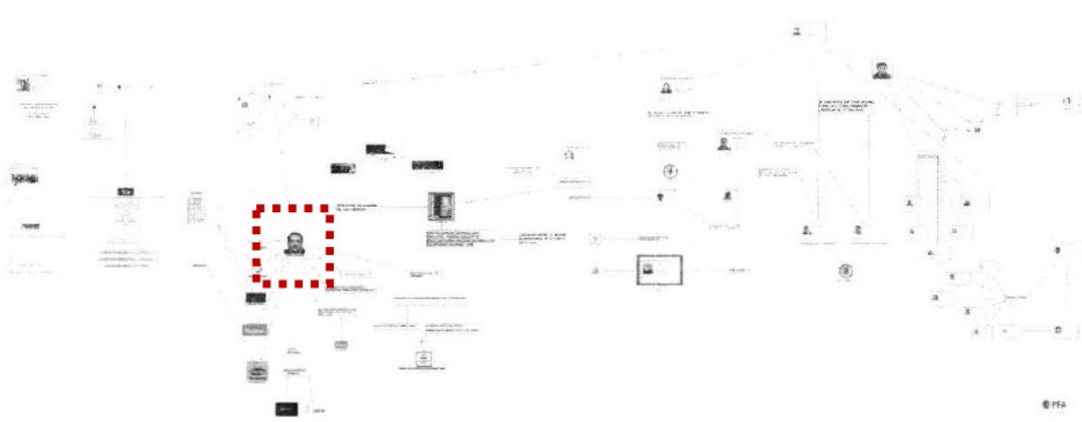
Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], conjuntamente con mi abogado defensor Pablo Slonimsqui, en la causa Nº 55.276/2019 caratulada *"NN S/VIOLACIÓN DE CORRESPONDENCIA"*, que tramita en la Secretaría n° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V. S. me presento y digo:

MANIFIESTA

En los dos (02) escritos presentado en este expediente por la defensa de E. V. C., **el 18 de mayo de 2021 y el 27 de mayo de 2021**, se solicitó a V. S. se le entregue copia del material de la investigación mencionado a fs. 1490-1502, que forma parte del legajo de prueba. **A tres (03) meses de esos pedidos**, ni el solicitante ni esta parte hemos tenido acceso aún a esos elementos.

En particular, y como expresé en el escrito presentado a V. S. el 15 de mayo de 2021, me intriga **el contenido del diagrama cuya miniatura se incluyó en el informe policial**,a fs. 555 vta. –elaborado por el **subcomisario Carlos Alberto Aguirre**, en el que sugiere a V. S. disponer de mi allanamiento, entre otros– en el que puedo reconocer la foto que aparece en mi DNI ubicada en un lugar central, **con múltiples flechas que parecen sugerir mi relación con otros sospechosos de esta causa**. Lo reproduzco a continuación con mi fotografía resaltada en línea punteada:



Dicho diagrama **no fue incluido de forma legible en el expediente** –se puso, como ya dije, apenas una miniatura borrosa– **ni aparece impreso en el abultado legajo de prueba**. Y al

parecer, por lo expresado a fs. 1682 por el fiscal Horacio Azzolin, **tampoco la Unidad Fiscal Especializada en Ciberdelincuencia pudo analizarlo**.

No puedo más que asumir que el diagrama en cuestión se encuentra entre los mencionados a fs. 1534-1535 del legajo de prueba, que fueron almacenados en el archivo de nombre "RESULTADO I2.zip"[1], que fue grabado en un CD o DVD marca "TDK" rotulado como "I2 Sumario N°785/19", depositado este último dentro de un sobre blanco rotulado "FS 1536 Legajo Prueba", y del que según consta a fs. 1490-1562 del expediente también se hizo una copia en un disco externo marca "Seagate" con número de serie "NAAD710K" que se encuentra el deposito de la Dirección de Prevención e Investigaciones de Delitos Tecnológicos de la Policía de la Ciudad de Buenos Aires.

Sin analizar ese diagrama no puedo defenderme. Necesito ver, como sí lo vieron otros para decidir sobre mi destino, cuál fue la hipótesis urdida por el **subcomisario Carlos Alberto Aguirre** para meterme en todo esto por la ventana. **Ya llevo esperando más de un (01) año y diez (10) meses.**

SOLICITA

En razón de lo expuesto, de V. S. solicito se me entregue copia del archivo "RESULTADO I2.zip" mencionado ut supra, contenido en el CD o DVD que forma parte de la fs. 1536 del legajo de prueba, **por considerarlo indispensable para ejercer mi derecho constitucional a la defensa**.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

1 Hash SHA-256: `2e109ce2d022f62d0f903325264ec7a28c7ccad63bf01d5fdab75625b228bebd`

MANIFIESTA – REITERA – SOLICITA

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], conjuntamente con mi abogado defensor Pablo Slonimsqui, en la causa Nº 55.276/2019 caratulada *"NN S/VIOLACIÓN DE CORRESPONDENCIA"*, que tramita en la Secretaría n° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V. S. me presento y digo:

MANIFIESTA

Que en el escrito presentado por esta parte el **01 de marzo de 2021** (fs. 1665-1670) solicité a V. S., entre otras cosas:

"1. Se expida precisando mi situación procesal.
2. Se formule imputación en mi contra y se me tome declaración indagatoria o, en su defecto,
3. se dicte mi sobreseimiento en esta causa.
4. Se impugne el uso del contenido de mi notebook como medio de prueba.
5. Se me devuelvan los elementos de trabajo que me fueran secuestrados."

Que en el escrito presentado por esta parte el **23 de abril de 2021** solicité a V. S., entre otras cosas:

"1. Se expida precisando mi situación procesal.
2. Se formule imputación en mi contra y se me tome declaración indagatoria o, en su defecto,
3. se dicte mi sobreseimiento en esta causa.
4. Se me devuelvan los elementos de trabajo que me fueran secuestrados indebidamente.
[...]
6. Se investigue lo denunciado por el fiscal Azzolin respecto de la vinculación de la amenaza de muerte recibida y la imagen de abuso sexual infantil intentando incriminarme."

Que en el escrito presentado por esta parte el **12 de agosto de 2021** solicité a V. S., entre otras cosas:

"1. Se me devuelvan mis herramientas con mis datos, toda vez que el trámite de lo actuado exhibe sin matices la ausencia de razones que justifiquen su secuestro.

2. Se me desvincule de esta causa, cesando en la afectación de mi buen nombre y honor.

[...]

4. Se investigue lo denunciado por el fiscal Horacio Azzolin respecto de la vinculación con esta causa de la amenaza de muerte recibida y la imagen de abuso sexual infantil intentando incriminarme."

Que por toda respuesta a estos pedidos, el Señor Fiscal dijo el **17 de septiembre de 2021**:

"En relación a lo manifestado por el señor Javier Lorenzo Carlos SMALDONE, respecto a la devolución de los efectos secuestrados en los allanamientos practicados, hágale saber que la presente investigación se encuentra en pleno trámite y restan producir varias medidas de prueba, por lo que entiendo que hasta el momento no podrá ser posible su restitución.

Por otro lado, en cuanto a la solicitud de originar una investigación respecto a lo manifestado por el Dr. Horacio AZZOLIN, hágase saber al presentante que del informe de colaboración, dicha denuncia se encuentra tramitando ante la Fiscalía Federal Nº 7."

Que aun entendiendo que V. S. ha delegado la instrucción de esta causa a la Fiscalía Federal n° 1, según lo normado por el art. 196 del CPPN, no debería ser el Sr. Fiscal quien resuelva sobre mi estado procesal ni sobre la devolución de mis herramientas de trabajo y mis datos, sino V. S.

Que por otra parte, es claro que del informe presentado por el Dr. Horacio Azzolin se desprende que la denuncia de amenazas por él recibidas está tramitando ante la Fiscalía Federal Nº 7, y de ninguna forma pediría a V. S. que se inmiscuya en dicha investigación. Lo que estoy solicitando, e insistiré en esto, es que se investigue cuál es la relación entre dichas amenazas y la causa de marras, que el propio Dr. Azzolin sugiere al decir *"La mención a Smaldone en el ataque a la Ministra Frederic y la burda atribución al nombrado de las amenazas que recibiera quien suscribe cuando ya se nos había dado intervención en el caso no patecen casuales"*. La relación sugerida por el titular de la UFECI, y no otra cosa, es lo que estoy pidiendo se investigue.

Que todo lo expuesto evidencia la situación de indefensión ya explicitada en presentaciones anteriores, como el escrito presentado por esta parte a fs. 1665-1670, causando un daño irreparable a mi persona. Tal daño se extiende a mi labor profesional, mi buen nombre y honor, así como también a la esfera personal, sujetándome a un proceso arbitrario e irrazonable que me impide el derecho de defensa amparado por nuestro plexo normativo.

REITERA – SOLICITA

En razón de lo expuesto, de V. S. solicito nuevamente:

1. Se expida precisando mi situación procesal.

2. Se formule imputación en mi contra y se me tome declaración indagatoria o, en su defecto,

3. se dicte mi sobreseimiento en esta causa.

4. Se me devuelvan los elementos de trabajo y los datos que me fueran secuestrados indebidamente.

5. Se investigue lo denunciado por el fiscal Azzolin respecto de la vinculación de esta causa con la amenaza de muerte y la imagen de abuso sexual infantil recibidas por él, y el ataque a la Ministra Sabina Frederic.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

MANIFIESTA – SOLICITA

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], conjuntamente con mi abogado defensor Pablo Slonimsqui, en la causa Nº 55.276/2019 caratulada *"NN S/VIOLACIÓN DE CORRESPONDENCIA"*, que tramita en la Secretaría n° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V. S. me presento y digo:

MANIFIESTA

Que habiendo podido acceder **–**después de casi dos años y luego de reiterados pedidos**–** a parte del material del legajo de prueba de esta causa relacionado con información obtenida a partir de mi línea telefónica (3586[redacted]), he podido comprobar fehacientemente una serie de irregularidades que detallo a continuación.

I - Obtención de llamadas y mensajes de texto entrantes y salientes de mi línea telefónica, incluyendo ubicación geográfica

A fs. 112 del expediente y fs. 429 del legajo de prueba aparece un pedido del **22 de agosto de 2019** del subcomisario Carlos Alberto Aguirre a V. S. que dice *"Atento a ello, pongo en su conocimiento que se destaco personal a realizar tareas investigativas a la provincia de Cordoba donde se pudo obtener información de relevancia para la presente causa, dentro de la cual se halla el abonado telefónico 3586*[redacted] *que estaría vinculado a una de los individuos pesquisados"*. Luego continúa Aguirre: *"Por lo expuesto y en razón de la sensibilidad de la causa que se investiga se solicita contemple el libramiento de ORDEN DE PRESENTACIÓN para la firma TELECOM ARGENTINA para el abonado 3586*[redacted] *respecto de los cuales deberán informar listado de llamadas Entrantes y salientes, las Antenas de activación del servicio y la Transferencia de Datos del abonado en cuestión desde el 01/07/2019 a la fecha, como asi también que aporten todos los datos con los que cuenten al momento de la registración del abonado"*.

¿De dónde obtuvo el personal policial ese número telefónico? ¿En qué consistieron las tareas investigativas? ¿En qué localidad o zona rural de la provincia de Córdoba se realizaron? ¿A qué individuo investigado estaría vinculado ese número? Nada de esto fue

dicho por Aguirre al pedir a V. S. que vulnere la garantía de las comunicaciones privadas, consagrada en el Artículo 19 de la Constitución Nacional.

Cabe destacar que número telefónico 3586[redacted] no aparece mencionado antes del pedido citado ut supra ni en el legajo de prueba ni mucho menos en el expediente de la causa.

El **4 de septiembre de 2019** el subcomisario Aguirre reiteró el pedido del 22 de agosto de 2019, sin agregar ningún dato adicional (fs. 922 del legajo de prueba, fs. 303 del expediente). Pero como puede verse en el reporte de geolocalización de la Policía Federal Argentina del 28 de agosto de 2019 (fs. 685-687 del legajo de prueba), en el que aparece mi nombre, los investigadores policiales ya sabían bien que la línea 3586[redacted] me pertenecía y habían obtenido su ubicación física.

¿Cómo supo el personal policial cuál es mi número telefónico? La respuesta parece ser el reporte incluido a fs. 691-696 obtenido de **"Sudamerica Data"**, un servicio accesible a través de la dirección `http://www.sudamericadata.com.ar/`. Una consulta a través del NIC Argentina permite determinar que ese sitio web está registrado a nombre del señor **Mario Fernando Ares** (CUIT 20-14[redacted]-2). ¿Es esta la fuente que usa la Policía Federal para determinar no sólo los números telefónicos asociados a un ciudadano, sino también información bancaria, financiera, patrimonial, laboral y de salud? Me resulta cuando menos curioso. Quizás esta es la razón por la que no dijeron a V. S. de qué forma habían obtenido el número telefónico del que requerían información.

A fs. 259 del expediente, el **5 de septiembre de 2019**, V. S. resolvió lo siguiente: *"En atención a lo solicitado por la División Investigación Delitos Tecnológicos de la P.F.A.. y a los efectos de proseguir obteniendo datos de interés que permitan individualizar a los autores del hecho que motiva la presente pesquisa, habré de librar orden de presentación, con allanamiento en subsidio, respecto de la firma Telecom Argentina S.A. para el día de la fecha, a partir de las 12 horas, a fin de que en forma urgente procedan a la inmediata entrega a la Instrucción del listado de llamadas entrantes y salientes, las antenas de activación del servicio, IMEI'S vinculados y transferencia de datos, todo ello en relación al abonado 358-6*[redacted]. *desde el día 01/07/2019 a la fecha"*.

¿Cómo se justificó esta medida? Así, sin más. Solo haciendo referencia al pedido policial, que tiene los vicios ya citados y carece de toda motivación. Curiosamente V. S. luego añadió tres extensos párrafos, citando los fallos "Urquía, Justo Ramón y otro s/ rec. de casación" (CNCP Sala II. c.n° 894, rto. El 28/02/1997), "Tellos. Eduardo A s/ recurso de casación" (Sala III, reg. n° 99) y "Balsas, Daniel y otros s/ rec. de casación" (Sala I. reg. n.º 437), citando fragmentos que ponen explicitan los criterios que debería tener en cuenta un magistrado al fundar una orden como esta. Precisamente, los que V. S. no consideró a la hora hacerlo.

II - Ampliación de la información sobre mis llamadas y mensajes telefónicos, incluyendo ubicación geográfica

Pero el avance sobre la privacidad de mis comunicaciones no se detuvo allí. En un pedido de fecha **16 de septiembre de 2019** (fs. 1318 del legajo de prueba, fs. 477 del expediente), el subcomisario Aguirre dice a V. S. *"Asimismo, y a modo de ampliación se solicita contemple el libramiento de ORDEN DE PRESENTACIÓN para la firma TELECOM ARGENTINA para el abonado 3586[redacted] respecto de los cuales deberán informar listado de llamadas Entrantes y salientes, IMEI vinculados, las antenas de activación del servicio y la Transferencia de Datos del abonado en cuestión desde el 01/05/2017 a la fecha, como así también que aporten todos los datos con los que cuenten al momento de la registración del abonado"*.

Nuevamente, como en el pedido original, no se dice ni cómo se obtuvo ese número, ni qué relación tendría con los hechos investigados, ni a quién pertenece. Como ya fue dicho, la Policía Federal ya sabía que dicho número era mío (por los datos dudosamente obtenidos de **"Sudamerica Data"**), y hasta a qué antena se conectaba, pero el subcomisario Aguirre ni siquiera necesitó decirlo para justificar su solicitud.

Ahora, resulta entendible que se pidan datos de una línea que se está investigando (con la debida justificación, que en este caso no existió) entre el 1 de julio y el 5 de septiembre de 2019, tratándose de un hecho que habría ocurrido entre el 20 de julio y el 14 de agosto del mismo año. **¿Pero cuál es el motivo para solicitar los datos desde el 1 de mayo de 2017? ¿Por qué los investigadores policiales necesitaban saber con quiénes yo había hablado o intercambiado mensajes y conocer mis movimientos, desde hacía más de dos años y cinco meses? ¿Y por qué esta medida no se pidió respecto de la otros más de cincuenta (50) números investigados?**

Nuevamente, aunque no hubo ninguna justificación para este pedido —ya completamente ilegítimo y desmedido—, V. S. respondió el **17 de septiembre de 2019** (fs. 479-480 del expediente): *"Por último, la empresa TELECOM deberá brindar asimismo todos los listados de llamadas entrantes y salientes del abonado 3586[redacted], desde el día 01/05/2017 a la fecha, incluyendo los IMEI vinculados, las antenas de activación del servicio y transferencia de datos, y toda la información con la que se cuente relativa al momento de la registración de aquél"*. Luego, añadió los mismos tres extensos párrafos ya referidos ut supra, detallando las consideraciones que debió tener al fundar dicha resolución, pero no tuvo.

III - Pedido de información a otros proveedores telefónicos y a WhatsApp

El mismo **16 de septiembre de 2019** (fs. 485 del expediente), el subcomisario Aguirre dijo a V. S.: *"En ese sentido, cumplo en informar que luego de un extenso análisis de la información*

aportada por la firma Telecom Personal S.A., se logró determinar que la linea 358-6[redacted] se encuentra vinculada al IMEI 3595[redacted]. Por lo narrado, solicito contemple el libramiento de Orden de Presentación a las firmas Telecom Personal S.A., AMX Claro S.A., y Telefónica Móviles S.A., a fin de que las mismas tengan a bien informar los abonados que impactaron en el Nº de IMEI antes mencionado, y en el caso de que sea positivo aporten listado de llamadas entrantes y salientes, IMEI asociados, impactos de antenas y transferencia de datos desde el 01/05/2017 a la fecha".

No conformes con averiguar con quiénes había tenido comunicaciones telefónicas durante los últimos dos años y cinco meses usando el número telefónico que obtuvieron de forma dudosa, la Policía Federal intentó saber también si había utilizado alguna otra línea. En este caso tampoco hubo ninguna justificación para el pedido, y nuevamente este se hizo sin mencionar el nombre de quien se estaba investigando.

En el mismo pedido, agregó Aguirre: *"Asimismo, se solicita el libramiento de oficio Judicial dirigido a la firma Whatsapp, a fin de que esa empresa tenga a bien aportar la totalidad de información incluyendo los log's de conexión, fecha de creación y correo electrónico asociado al abonado telefónico 358-6[redacted]. desde el 01/05/2017 a la fecha".*

Así intentó también la policía conocer los datos de mi cuenta y mis comunicaciones de los últimos dos años y cinco meses a través del sistema de mensajería WhatsApp, medida que no se tomó con nadie más. Y nuevamente, sin decir cuál sería el interés para la causa, quién sería el investigado y por qué debería permitírseles acceder a esta información.

Y V. S. respondió a este pedido el **18 de septiembre de 2019** (fs. 496-497) avalando este pedido totalmente abusivo e infundado.

IV – La violación de la privacidad de mis comunicaciones telefónicas y de terceros

En el informe de la empresa Telecom Personal S. A. recibido por la policía el 19 de septiembre de 2019 según fs. 1385 del legajo de prueba, y que consta en el CD que forma parte de la fs. 1380 del mismo, el prestador telefónico entregó un total de **treinta y cuatro (34) planillas** de cálculo (.xls), veintinueve (29) de ellas detallando todo el tráfico de datos y cinco (05) con el total de llamadas entrantes y salientes de la línea telefónica 3586[redacted] de mi propiedad **entre las fechas 1 de mayo de 2017 y 16 de septiembre de 2019**. Sí, el detalle completo de mis desplazamientos físicos y mis llamadas telefónicas durante **ochocientos sesenta y nueve (869) días**, incluyendo **treinta y nueve mil quinientos ochenta y siete (39.587) conexiones a celdas de telefonía** y **siete mil setecientos treinta y un (7.731) llamadas**, en todos los casos con su ubicación geográfica exacta. Esa fue la magnitud de la violación de mi privacidad, realizada de forma completamente injustificada e infundada.

Además, Telecom Personal S. A. entregó –excediendo la ya infundada manda judicial– los datos personales de **noventa y siete (97) personas, setenta y cinco (75) de ellas físicas y veintidós (22) jurídicas**, incluyendo nombre completo, CUIT o DNI, domicilio y número de teléfono fijo. Los efectivos policiales, lejos de denunciar esta violación masiva de la privacidad, decidieron cargar y procesar estos datos personales en su herramienta inteligencia (espionaje) "IBM i2", hecho que queda de manifiesto al observar el diagrama "LINEAS INVESTIGADAS JUNTAS.anb" que se encuentra en el CD que forma parte de la fs. 1536 del legajo de prueba.

V - Conclusión

Los investigadores policiales, bajo la supervisión del subcomisario Carlos Alberto Aguirre, solicitaron a V. S. ordene la obtención del detalle de llamadas entrantes y salientes, de mensajes de texto y de tráfico de datos, incluyendo en todos los casos la ubicación geográfica de mi teléfono celular, por un plazo completamente excesivo de **dos (02) años, cuatro (04) meses y dieciséis (16) días**, **sin esgrimir ni el motivo concreto por el que se motivaba tal pedido, de dónde se obtuvo el número telefónico en cuestión y sin siquiera decir quién sería su titular**. Esto, sumando además el pedido de datos a la empresa WhatsApp, **no se hizo con ningún otro de los investigados**. V. S. hizo lugar a las medidas solicitadas de forma completamente infundada.

El resultado, sumado al exceso cometido por la empresa Telecom Personal S.A. convenientemente aprovechado por los investigadores policiales, fue una violación masiva de mi privacidad y de la confindencialidad de mis comunicaciones, llegando al extremo de afectar a terceros que nada tuvieron ni tienen que ver con la causa de marras.

SOLICITA

En razón de lo expuesto, de V. S. solicito:

1. Se forme incidente de estilo, y oportunamente se declare la nulidad de los pedidos de información sobre el número telefónico 3586[redacted] y del IMEI 3595[redacted], y demás actos procesales consecuentes, incluyendo toda prueba derivada de los mismos.
2. Se ordene la correspondiente extracción de testimonios a los fines de investigar los ilícitos mencionados en este escrito, en particular el hostigamiento y los abusos que sufrí por parte del personal policial, en cabeza del subcomisario Carlos Alberto Aguirre.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

INSISTE.

Sr. Juez:

Pablo Slonimsqui, por la representación que ostento, en la causa que lleva el nº 55276/2019 del registro de la Secretaría nº 18 de este Juzgado Nacional en lo Criminal y Correccional Federal nº 9, ante V.S. me presento y digo:

Que tomado conocimiento de lo dispuesto por el Tribunal en el día de la fecha, y estimo imprescindible formular las siguientes consideraciones.

Así, puesto que al dar respuesta —que se agradece— a dos presentaciones oportunamente concretadas por esta defensa, V.S. manifestó, en la relación con la primera de ellas, que "*mientras esta sede se encontró a cargo de la instrucción de los autos principales CCC 55276/2019, se asignó el debido trámite a la petición de nulidad efectuada por dicho letrado, en relación a la orden por la que hubo de disponerse el registro domiciliario de su defendido, en base a las evidencias y los informes policiales previamente glosados en el legajo. En efecto, en la incidencia (n° 3) formada en consecuencia, la Sala II de la Excma. Cámara del fuero -con fecha 14 de febrero de 2020-, hubo de confirmar en un todo el decisorio adoptado por quien suscribe. A su vez, y con posterioridad a ello, la Sala III de la Excelentísima Cámara Federal de Casación Penal -con fecha 19 de agosto de 2020-, declaró mal concedido el recurso de casación interpuesto por el letrado aludido, contra la aludida resolución de la Sala II de la Alzada de este fuero*".

Y en cuanto se vincula con la entrega de los elementos que fueran incautados en el domicilio de mi defendido, señaló V.S. que "*en estricto cumplimiento de lo decidido por la propia Alzada, el 14 de febrero de 2020 -en la incidencia formada oportunamente a tal fin (n° 4)-, la Fiscalía Federal n° 1 que interviene, el 21 de enero del corriente año y ya a cargo de la pesquisa en virtud de lo normado por el art. 196 del ritual, hubo de efectivizar la entrega de diversos elementos a la incidentista* [redacted]*. Se asume que su titular, de considerarlo pertinente, habrá de avocarse al tratamiento de las cuestiones ahora introducidas*".

En este escenario, y de conformidad con la delegación de la instrucción dispuesta en autos con fecha 18 de diciembre de 2019, V.S. dispuso remitir "*el libelo acompañado a la mencionada representación Fiscal, a los efectos que allí estime corresponder y con ajuste al estado en que se hallen las actuaciones; ello, toda vez que el Tribunal se encuentra impedido de obrar de cualquier otro modo, bajo la estricta observancia de las facultades acusatorias que impone la normativa aludida: 'No puede dejar de recordarse que este instituto tiende, además,*

a dar virtualidad al principio acusatorio, ya que amplía las posibilidades del que el Fiscal investigue. Un modelo de enjuiciamiento acorde con estas pautas es una garantía del individuo y no de los órganos del Estado, cuyas disputas no debieran afectarle. Al mismo tiempo, la introducción del artículo 120 en la Constitución Nacional, si alguna modificación produjo al paradigma procesal fue justamente a favor de una separación mucho más estricta de las funciones de acusar y juzgar (Fallos 327:5863), por lo que no se comprende la existencia de un agravio a raíz de una disposición que contribuye justamente con dicha separación -ver causa n° 45.212, rta. 10/02/2011, reg. n° 66, entre otras- (CCCF – Sala I - CFP 7917/19/1/RH1 - Juzgado n° 12 - Secretaría n° 23, Rta. 10/03/2020)'."

En este marco, entonces, habré de formular las siguientes aclaraciones:

1 Mediante uno de los mencionados escritos se reclama la devolución de los elementos de trabajo que hace ya mas de dos años le fueran secuestrados a mi defendido, de momento nadie sabe bien por qué ni para qué. Nada obsta a la prosperidad de este planteo el hecho que oportunamente le hayan sido devueltos otros elementos secuestrados a [redacted]. Puesto que si bien es cierto que este planteo fue rechazado por V.S. anteriormente, no lo es menos que ha transcurrido un tiempo incomprensible sin que el Ministerio Público resuelva qué hacer con los mencionados elementos. Por esta razón, en la inteligencia que mi defendido esta siendo víctima de un proceder arbitrario en cabeza de su adversario procesal, es que nuevamente se reclama la intervención de V.S. que, como se dijo, resulta ser en definitiva el único garante de los derechos y garantías que asisten al Sr. Smaldone.

   Así, es el incomprensible tiempo muerto que exhibe el legajo desde que V.S. resolviera la cuestión el que autoriza a esta parte a insistir con su postura. Porque parece evidente que en autos no se hizo lugar —en su momento— a la devolución de los efectos que aquí se reclaman por resultar los mismos de interés para la investigación, cuestión que aparece hoy desmentida por los hechos.

2 En relación con el segundo de los escritos, señaló esta parte que habiendo podido acceder —después de casi dos años y luego de reiterados pedidos— a parte del material del legajo de prueba de esta causa relacionado con la información obtenida a partir de la línea telefónica (3586[redacted]), se habían podido comprobar fehacientemente una serie de irregularidades.

   En cuanto aquí interesa, pudimos conocer la existencia de un pedido de fecha 16 de septiembre de 2019 (fs. 1318 del legajo de prueba, fs. 477 del expediente), ocasión en la que el subcomisario Aguirre dice a V. S. *"Asimismo, y a modo de ampliación se solicita contemple el libramiento de ORDEN DE PRESENTACIÓN para la firma TELECOM*

ARGENTINA para el abonado 3586[redacted] respecto de los cuales deberán informar listado de llamadas Entrantes y salientes, IMEI vinculados, las antenas de activación del servicio y la Transferencia de Datos del abonado en cuestión desde el 01/05/2017 a la fecha, como así también que aporten todos los datos con los que cuenten al momento de la registración del abonado".

Sin la menor aclaración acerca de cómo se obtuvo ese número, ni qué relación tendría con los hechos investigados, ni a quién pertenecía, y sin dejar de ver que, con algún esfuerzo, podría resultar entendible que se pidan datos de una línea que se está investigando (con la debida justificación, que en este caso no existió) entre el 1 de julio y el 5 de septiembre de 2019 (tal como se hizo inicialmente con este número y con el resto de los investigados), tratándose de un hecho que habría ocurrido entre el 20 de julio y el 14 de agosto del mismo año. **Pero lo que en modo alguno encuentra explicación racional refiere al motivo —o la falta de motivos— invocados para solicitar los datos mencionados desde el 1 de mayo de 2017.** ¿Por qué los investigadores policiales necesitaban saber con quiénes el Sr. Smaldone había hablado o intercambiado mensajes y conocer sus movimientos, desde hacía más de dos años y cinco meses? ¿Y por qué esta medida no se pidió respecto de la otros más de cincuenta (50) números investigados?

Nuevamente, aunque no hubo ninguna justificación para este pedido —ya completamente ilegítimo y desmedido—, V. S. respondió el 17 de septiembre de 2019 (fs. 479-480 del expediente): *"Por último, la empresa TELECOM deberá brindar asimismo todos los listados de llamadas entrantes y salientes del abonado 3586[redacted], desde el día 01/05/2017 a la fecha, incluyendo los IMEI vinculados, las antenas de activación del servicio y transferencia de datos, y toda la información con la que se cuente relativa al momento de la registración de aquél"*.

El mismo 16 de septiembre de 2019 (fs. 485 del expediente), el subcomisario Aguirre dijo a V. S.: *"En ese sentido, cumplo en informar que luego de un extenso análisis de la información aportada por la firma Telecom Personal S.A., se logró determinar que la linea 358-6[redacted] se encuentra vinculada al IMEI 3595[redacted]. Por lo narrado, solicito contemple el libramiento de Orden de Presentación a las firmas Telecom Personal S.A., AMX Claro S.A., y Telefónica Móviles S.A., a fin de que las mismas tengan a bien informar los abonados que impactaron en el N° de IMEI antes mencionado, y en el caso de que sea positivo aporten listado de llamadas entrantes y salientes, IMEI asociados, impactos de antenas y transferencia de datos desde el 01/05/2017 a la fecha"*.

No conformes con averiguar con quiénes había tenido mi defendido comunicaciones telefónicas durante los últimos dos años y cinco meses usando el número telefónico que

obtuvieron de forma dudosa, la Policía Federal intentó saber también si el Sr. Smaldone había utilizado alguna otra línea. En este caso tampoco hubo ninguna justificación para el pedido, y nuevamente este se hizo sin mencionar el nombre de quien se estaba investigando.

En el mismo pedido, agregó Aguirre: *"Asimismo, se solicita el libramiento de oficio Judicial dirigido a la firma Whatsapp, a fin de que esa empresa tenga a bien aportar la totalidad de información incluyendo los log's de conexión, fecha de creación y correo electrónico asociado al abonado telefónico 358-6[redacted]. desde el 01/05/2017 a la fecha"*.

Así intentó también la policía conocer los datos de la cuenta de mi defendido y sus comunicaciones de los últimos dos años y cinco meses a través del sistema de mensajería WhatsApp, medida que no se tomó con nadie más. Y nuevamente, sin decir cuál sería el interés para la causa, quién sería el investigado y por qué debería permitírseles acceder a esta información.

Y V. S. respondió a este pedido el 18 de septiembre de 2019 (fs. 496-497) avalando este pedido totalmente abusivo e infundado.

En el informe de la empresa Telecom Personal S. A. recibido por la policía el 19 de septiembre de 2019 según fs. 1385 del legajo de prueba, y que consta en el CD que forma parte de la fs. 1380 del mismo, el prestador telefónico entregó un total de treinta y cuatro (34) planillas de cálculo (.xls), veintinueve (29) de ellas detallando todo el tráfico de datos y cinco (05) con el total de llamadas entrantes y salientes de la línea telefónica 3586[redacted], propiedad del Sr. Smaldone, entre las fechas 1 de mayo de 2017 y 16 de septiembre de 2019. Sí, el detalle completo de sus desplazamientos físicos y sus llamadas telefónicas durante ochocientos sesenta y nueve (869) días, incluyendo treinta y nueve mil quinientos ochenta y siete (39.587) conexiones a celdas de telefonía y siete mil setecientos treinta y un (7.731) llamadas, en todos los casos con su ubicación geográfica exacta. Esa fue la magnitud de la violación de su privacidad, realizada de forma completamente injustificada e infundada.

Además, Telecom Personal S. A. entregó –excediendo la ya infundada manda judicial– los datos personales de noventa y siete (97) personas, setenta y cinco (75) de ellas físicas y veintidós (22) jurídicas, incluyendo nombre completo, CUIT o DNI, domicilio y número de teléfono fijo. Los efectivos policiales, lejos de denunciar esta violación masiva de la privacidad, decidieron cargar y procesar estos datos personales en su herramienta inteligencia (espionaje) "IBM i2", hecho que queda de manifiesto al observar el diagrama "LINEAS INVESTIGADAS JUNTAS.anb" que se encuentra en el CD que forma parte de la fs. 1536 del legajo de prueba.

A modo de corolario, podemos ver que los investigadores policiales, bajo la supervisión del subcomisario Carlos Alberto Aguirre, solicitaron a V. S. ordene la obtención del detalle de llamadas entrantes y salientes, de mensajes de texto y de tráfico de datos, incluyendo en todos los casos la ubicación geográfica del teléfono celular de mi defendido, por un plazo completamente excesivo de dos (02) años, cuatro (04) meses y dieciséis (16) días, sin esgrimir ni el motivo concreto por el que se motivaba tal pedido, de dónde se obtuvo el número telefónico en cuestión y sin siquiera decir quién sería su titular. Esto, sumando además el pedido de datos a la empresa WhatsApp, no se hizo con ningún otro de los investigados. V. S. hizo lugar a las medidas solicitadas de forma completamente infundada.

En este escenario, parece notorio, ostensible y manifiesto que el planteo de nulidad oportunamente interpuesto en relación con los hechos *supra* descriptos es completamente diferente de aquel resuelto oportunamente por V.S.

Podrá esta defensa tener razón o no, eso ya se verá, pero de lo que no existe la menor duda es de que se trata de planteos distintos, en este último caso, cimentado sobre la evidencia de que por razones que se desconocen —pero pueden imaginarse— el personal policial utilizó este legajo para colectar información reservada respecto de mi defendido, en referencia con períodos que bajo ningún punto de vista pueden considerarse incluidos dentro del objeto procesal de las presentes actuaciones.

Caso contrario, sería de suma importancia para la transparencia que debe lucir toda investigación criminal, que alguien explique con un lenguaje sencillo, que todos podamos fácilmente comprender, cuales han sido las razones por las que se ha obtenido información sensible de mi defendido *desde el 01 de mayo de 2017, cuando el hecho investigado* habría ocurrido entre el 20 de julio y el 14 de agosto de 2019.

Queda claro entonces que el planteo nulificante ya resuelto en autos se vincula con la fundamentación de la orden de allanamiento oportunamente dictada respecto del domicilio del Sr. Smaldone, y el presente planteo refiere a la absoluta ilegitimidad de exhibe la incorporación de información sensible vinculada con el nombrado, que se corresponde con el periodo alcanzado entre las fechas 1 de mayo de 2017 y 16 de septiembre de 2019.

Por las razones expuestas, esta defensa entiende que debe V.S., en su rol de director del proceso, avocarse al conocimiento de las dos cuestiones planteadas por esta defensa, formando los incidentes de estilo.

Proveer de conformidad,

SERÁ JUSTICIA.

MANIFIESTA - SOLICITA

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI Nº [redacted], conjuntamente con mi abogado defensor Pablo Slonimsqui, en la causa Nº 55.276/2019 caratulada *"NN S/VIOLACIÓN DE CORRESPONDENCIA"*, que tramita en la Secretaría n° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n° 9, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V. S. me presento y digo:

MANIFIESTA

Que habiendo finalmente podido acceder –luego de más de dos (02) años y reiterados pedidos– a los diagramas mencionados como "ANEXO 1", "ANEXO 2" y "ANEXO 3" en el informe policial de fs. 555-558, en el que se basaron los numerosos allanamientos y detenciones dispuestos por V. S. a fs. 591-606, he logrado lo que a estas alturas creía imposible: sorprenderme aún más.

0. - Sobre los "anexos" del informe policial

Los anexos en cuestión, que son solamente mencionados en el informe policial que tiene como conclusión la necesidad de las medidas mencionadas, no están incluidos ni en el expediente principal de esta causa ni tampoco en el legajo de prueba digitalizado y publicado en el sistema informático LEX 100, sino que se encuentran dispersos en una variedad de lugares y formatos. En particular, respecto de los formatos, deberemos distinguir:

- **Archivos ANB**: Son archivos con diagramas generados desde la herramienta de análisis criminalístico "IBM i2", utilizada por los agentes policiales para reunir la información de la investigación (llamadas telefónicas, datos de los sospechosos y otras personas vinculadas, etc.). Estos archivos pueden ser solamente visualizados, para lo que se requiere un programa especial gratuito de la empresa IBM.

- **Archivos PNG**: Son archivos en un formato gráfico de representación de imágenes, visualizables con software de uso general.

- **Láminas impresas**: Son diagramas impresos en láminas de papel continuo de 61 cm de ancho, y su largo depende de la extensión de los mismos.

Para poder analizar uno de estos diagramas en detalle es indispensable contar con el archivo ANB (y la herramienta gratuita correspondiente), que incluye no solo información

visual, sino también datos asociados a los elementos que los integran. Los archivos PNG, si tienen una resolución y un tamaño razonable, permiten al menos visualizar los componentes gráficos del diagrama. Las láminas impresas resultan por demás inconvenientes (al punto que me llevó más de dos años poder acceder a ellas, debiendo desplazarme físicamente a la fiscalía para observarlas y fotografiarlas por partes). Solo en caso del "ANEXO 2" se incluyó en el expediente (a fs. 555 vta.) una miniatura de pequeñas dimensiones, completamente ilegible.

Los archivos que sí fueron aportados, se encuentran dispersos en distintos medios entre la "evidencia digital" guardada en sobres que fueron reunidos y enviados en su oportunidad a la Policía de la Ciudad, según consta en el acta de fs. 1490-1502. En particular, en los ítems numerados como "51" y "54":

- Ítem 51:
  Archivo: "RESULTADO I2.zip"
  SHA256: `a52b41de1d8fce6324a93485c225bl702756150eb65dee982ff07b8fcbf5efb2`
  Contenido:
    "1 - LINEA DE TIEMPO.anb"
    "2 - LINEAS INVESTIGADAS JUNTAS.anb"
    "3 - LINEAS INVESTIGADAS JUNTAS – VINCULOS.anb"

- Ítem 54:
  Archivo: "LINEA DE TIEMPO.png"
  SHA256: `d4bd77ca8bedf34e73b59a4b7b3d2791cc3c647216584d5ebc7aec42463b7836`

En definitiva, esta es la mixtura de formatos en que se presentaron los tres (03) anexos:

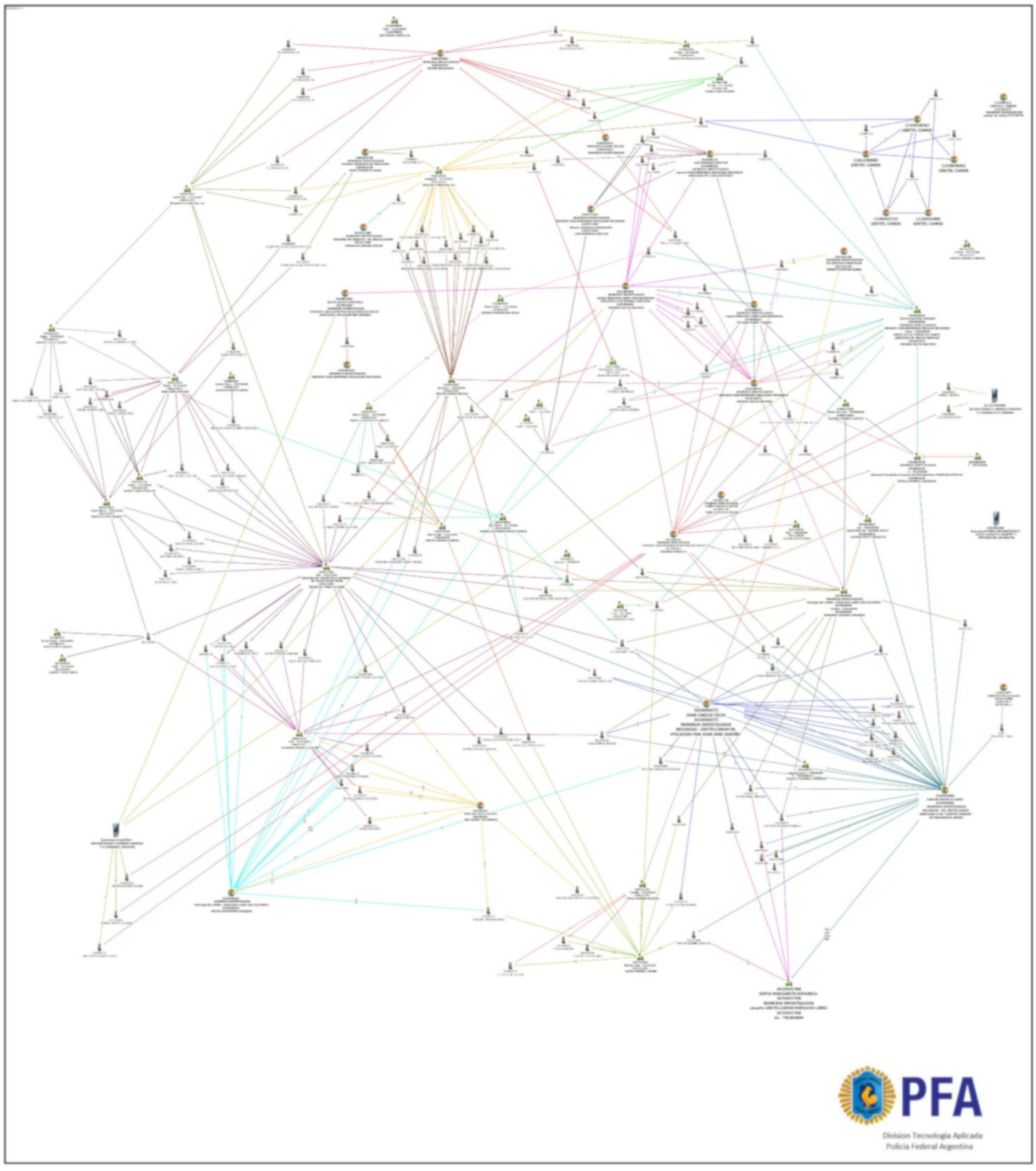
	Expediente	**Archivo ANB**	**Archivo PNG**	**Lámina**
ANEXO 1	NO	"3 - LINEAS INVESTIGADAS JUNTAS - VINCULOS.anb"	NO	SÍ
ANEXO 2	Miniatura	NO	NO	SÍ
ANEXO 3	NO	"1 - LINEA DE TIEMPO.anb"	"LINEA DE TIEMPO.png"	NO

No se entiende ni se explica –pero sí se sospecha– por qué los investigadores no aportaron los archivos ANB y los gráficos PNG de los tres (03) anexos en cuestión, cuando evidentemente disponían de ellos, realizando en cambio una mezcla que a todas luces dificulta el acceso a los mismos, así como su análisis y comprensión.

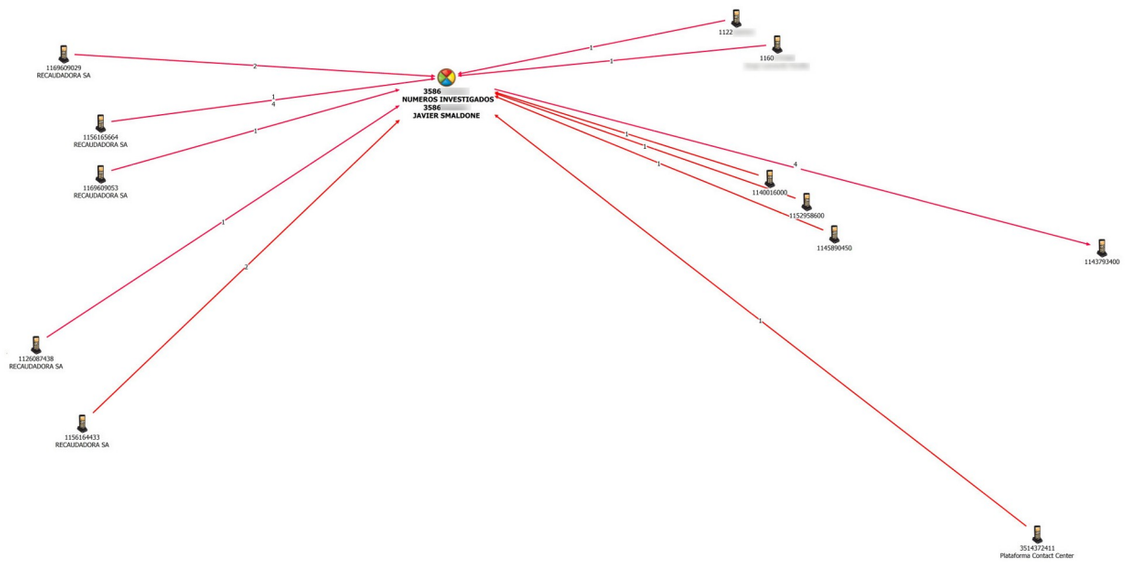
A fin de enmendar –tarde y en parte– esta clara deficiencia de la instrucción, reproduciré a continuación los fragmentos de dichos diagramas que se relacionan con mi persona, reconstruidos con gran esfuerzo, y luego dedicaré algunas breves reflexiones respecto de su contenido.

1.- El “ANEXO 1”

En este diagrama los investigadores policiales intentaron mostrar las supuestas vinculaciones entre los distintos actores, a través de llamadas telefónicas realizadas y recibidas por los mismos. En todos los casos se incluyeron datos de entre julio y septiembre de 2019, pero solo en mis caso se añadieron datos desde mayo de 2017. Así luce una miniatura del diagrama mencionado como “ANEXO 1” a fs. 555 (generado a partir del archivo “3 - LINEAS INVESTIGADAS JUNTAS – VINCULOS.anb” aportado por la Policía Federal).



Visto así, resulta una red donde en apariencia todos tienen que ver con todos, pero si seleccionamos solo la parte que tiene que ver conmigo, obtenemos lo siguiente:



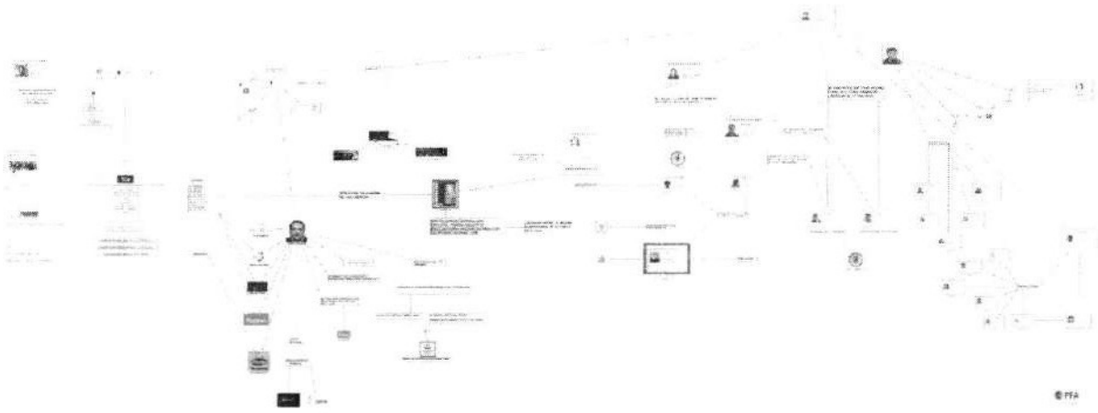
¿Qué dice esto? Que en el transcurso de dos (02) años y cinco (05) meses recibí unas once (11) llamadas de una empresa llamada “RECAUDADORA S.A”, una (01) llamada de “Plataforma Contact Center”, que cuatro (04) veces llamé al número 1143793400 de la tarjeta de crédito VISA. Que también recibí una (01) llamada del número 1140016000, una (01) del 1152958600 y una (01) del 1145890450, tres números que tras una rápida búsqueda en Internet están reportados como pertenecientes a distintos call centers. Todas llamadas con empresas.

Y también habría recibido una (01) llamada del número 1122[redacted] y una (01) del número 1160[redacted]. Esto, según el diagrama de los investigadores policiales, me vincularía con un tal “C[redacted]”, que aparecería entre los que se comunicaron por Telegram con quien a su vez sería el autor de la filtración investigada, porque también lo llamaron una (01) y cinco (05) veces, respectivamente. Esto es, volviendo al diagrama “ANEXO 1”:

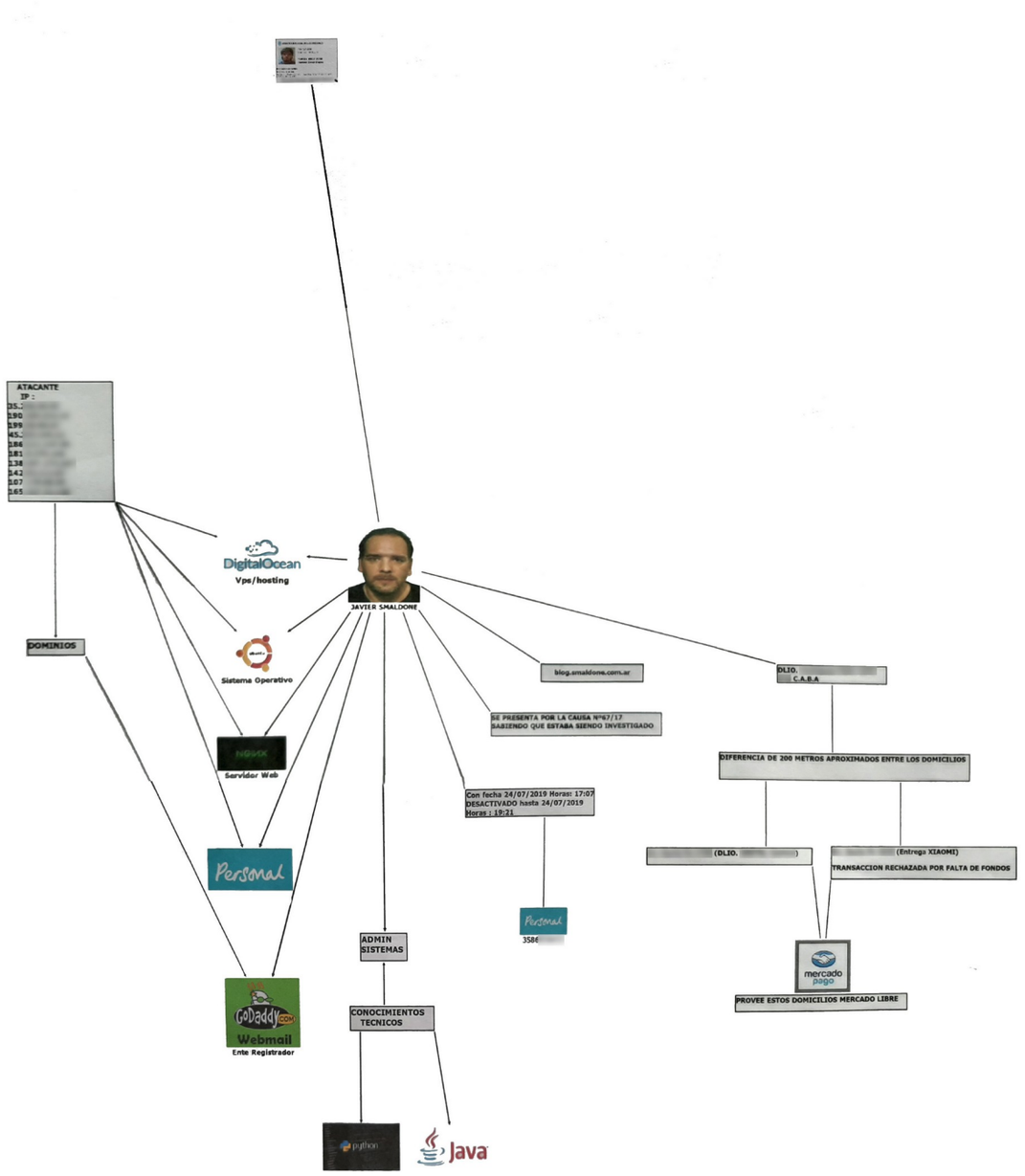
¿Esto es lo que obtuvieron como indicio de mi participación en los hechos investigados luego de analizar mis llamadas telefónicas y tráfico de datos, incluyendo la ubicación geográfica, durante dos (02) años y cinco (05) meses?

2.- El “ANEXO 2”

En este diagrama los investigadores policiales intentaron mostrar un panorama general con todos los actores involucrados en la investigación y sus supuestas relaciones. Así luce una miniatura del diagrama mencionado como “ANEXO 2” a fs. 555 vta. del expediente:



Como ya fue dicho, los agentes policiales no aportaron ni el archivo ANB generado por el software “i2”, ni una imagen del mismo en formato PNG de este diagrama. A continuación, muestro la parte que tiene que ver conmigo, y que tuve que reconstruir a partir de la unión de las fotografías que tomé del mismo en la fiscalía:



Así, resulta que aparezco en medio de un diagrama gigantesco –que vincula a no menos de veinticinco personas– porque:

1 Se relaciona las direcciones IP que supuestamente intervinieron en el ataque a la Policía Federal conmigo por la coincidencia de algún software (Ubuntu, nginx) o proveedor de servicios (Digital Ocean, GoDaddy, Telecom Personal). Esto es completamente descabellado, aún para quien no entienda nada de informática.

2 Tengo conocimientos de programación y administración de sistemas informáticos. Reconozco ser culpable de esto, a la vez que quien exhibe esto como motivo de sospecha es completamente inocente.

3 Cierto día apagué mi celular o me quedé sin señal durante unas dos horas. ¿A quién no le pasó?

4 Mi domicilio en la Ciudad de Buenos Aires está a unos 200 metros de donde se habría comprado un celular usado para el ataque. En una de las áreas de mayor actividad comercial del país.

5 Hay una línea trazada entre mi fotografía y la de [redacted], sin ninguna etiqueta ni explicación.

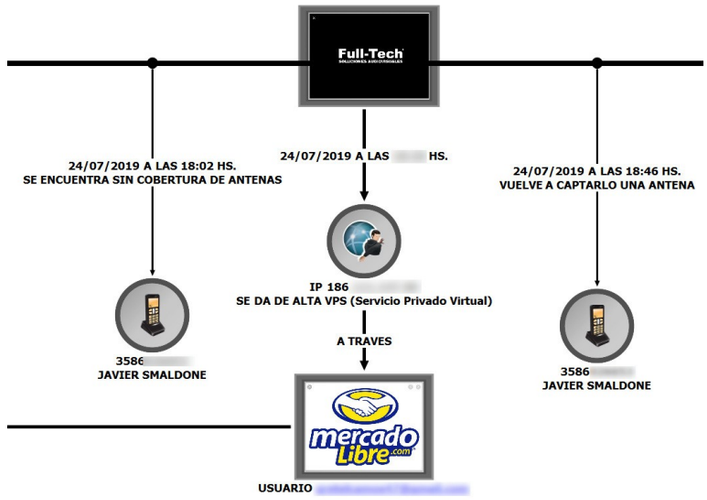
6 Tengo un blog.

7 Me presenté en una causa anterior al enterarme de que había sido investigado –sin motivo y sin resultar en ninguna imputación– por la misma fuerza policial que realizó este diagrama. Omitiendo decir que además presenté prueba y declaración testimonial, como ya quedó probado con el acta que consta a fs. 1162-1164.

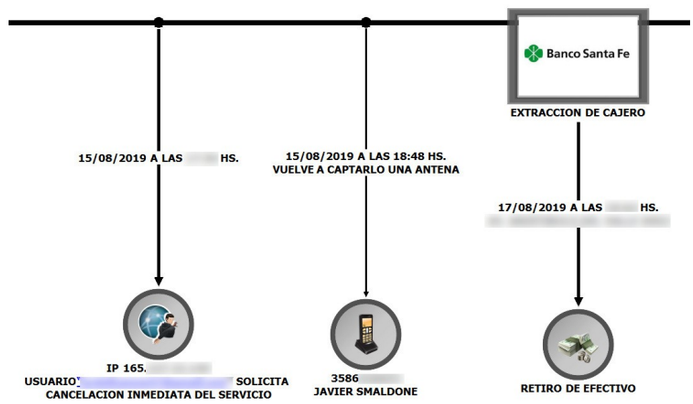
Debo recordar aquí las consideraciones que este tipo de argumentos motivaron por parte del titular de la UFECI, el fiscal Horacio Azzolin, que en su dictamen de fs. 1681-1692 fue desde tildar este tipo de argumentos como “no científicos” hasta compararlos con los utilizados en la dictadura militar. Lo puedo decir más fuerte pero no más claro: **esto es un mamarracho, y este tipo de argumentos no deberían poder usarse para incriminar a nadie**.

3.- El “ANEXO 3”

En este diagrama los investigadores policiales muestran una serie eventos supuestamente relacionados con los hechos investigados en una línea de tiempo, según se dijo a fs. 556. A continuación extraigo los dos fragmentos de este extenso gráfico, tomados del archivo PNG “LINEA DE TIEMPO.png” aportado por la Policía Federal:



En qué se relacionaría con los hechos que mi celular se haya quedado sin cobertura de antenas (quizás por estar apagado, por estar en un sótano o alguna otra área sin señal) mientras alguien daba de alta un servidor desde el que luego presumiblemente se realizaría el ataque a la Policía Federal. Una estupidez.



Y otra vez la misma estupidez. Un día alguien cancela el servidor antes mencionado, y al día siguiente se restablece la conexión de mi teléfono celular (que no se dice cuándo se habría interrumpido). Y un día después, alguien retira dinero de un cajero automático en la ciudad de Santa Fe.

¿A esto se reduce mi supuesta participación en este grave hecho delictivo a través del tiempo?

4.- Conclusión

Un mamarracho tras otro, presentados de forma de dificultar el acceso a los mismos. Seguramente estos tres (03) diagramas fueron mostrados al Tribunal a la hora se sugerir que allanaran mi domicilio y secuestraran mis herramientas de trabajo (conteniendo mis datos). Pero evidentemente no fueron vistos por nadie con dos dedos de frente (seguramente no por la Unidad Fiscal Especializada en Ciberdelincuencia).

SOLICITA

En virtud de lo expuesto, de V. S. solicito:

1 Se requiera a la Policía Federal Argentina que aporte la versión digital original (archivo en formato ANB) del diagrama mencionado como “ANEXO 2” en el informe de fs. 555-558, que solo fue entregado impreso en una lámina.

2 Anticipando que V. S. y el fiscal actuante se disculparán de adentrarse en la lectura de mis argumentos por juzgarlos “técnicos”, se envíen los diagramas mencionados en el informe policial de fs. 555-558 como “ANEXO 1”, “ANEXO 2” y “ANEXO 3” (en sus versiones digitales cuando fuera posible, o impresas en caso contrario) junto con el presente escrito a la Unidad Fiscal Especializada en Ciberdelincuencia para su análisis y evaluación.

Proveer de conformidad SERÁ JUSTICIA.

Javier Lorenzo Carlos Smaldone

FINISH WHAT YOU STARTED – ADJUNTA

> *"Mi dibujo no representaba un sombrero. Representaba una serpiente boa que digería un elefante. Dibujé entonces el interior de la serpiente boa a fin de que las personas grandes pudiesen comprender. Siempre necesitan explicaciones."*
>
> *(Antoine de Saint-Exupéry, "El Principito")*

Señor Juez Federal:

Javier Lorenzo Carlos Smaldone, DNI n.º [redacted], conjuntamente con mi abogado defensor Pablo Slonimsqui, en la causa CCC 55276/2019 caratulada *"NN S/VIOLACIÓN DE CORRESPONDENCIA"*, que tramita en la Secretaría n.° 18 del Juzgado Nacional en lo Criminal y Correccional Federal n.° 9, manteniendo el domicilio constituido en [redacted] de esta Ciudad Autónoma de Buenos Aires (domicilio electrónico [redacted]), ante V.S. me presento y digo:

Que el sobreseimiento dictado a mi respecto ha quedado firme.

Se trata de una resolución ajustada a derecho, dejando de lado que el Tribunal demoró aproximadamente dos años en dictarla.

A **fs. 1665-1669** presenté un escrito detallando las inconsistencias, falsedades y contradicciones de la investigación policial, que fue ampliado por los presentados a **fs. 1677-1678**, **fs. 1693-1701** y el **23 de abril de 2021**, pidiendo a V.S. en todos los casos que investigue los posibles ilícitos y omisiones cometidos por el personal a cargo de la misma.

Que ninguno de estos pedidos fue nunca satisfecho por V.S.

Desde esa perspectiva, entiendo que lo resuelto no refleja *in totum* las conclusiones que exhibe el legajo.

Por lo demás, el archivo dispuesto también permite concluir que los verdaderos autores de la maniobra que debió ser investigada se irán de rositas, y aquí no ha pasado nada.

Queda para el recuerdo, en definitiva, un expediente desopilante, que incluye distintos episodios inconcebibles, como ser el tratamiento que se dio a los efectos personales que se secuestraran en mi domicilio, el sketch del exhorto con destino a los Estados Unidos de América, o la busqueda del tesoro que debimos enfrentar los imputados para encontrar el escondite donde se hallaban las pruebas que supuestamente nos incriminaban.

En otro orden de cosas, interesa señalar en esta despedida que he observado que a lo largo de este proceso se ha dado entidad a múltiples diagramas elaborados por los investigadores de la Policía Federal Argentina —algunos de los cuales no me fueron mostrados sino hasta

transcurridos más de 2 años de mi allanamiento. Evidentemente la representación gráfica resulta más asequible para el Tribunal.

En virtud de esto, me parece apropiado adjuntar al presente escrito un diagrama en forma de línea de tiempo, resaltando los hechos descriptos en los libelos mencionados ut supra, que elaboré en el convencimiento de que sería de utilidad ante la improbable eventualidad de que los gravísimos sucesos verificados en estos autos sean investigados con el rigor profesional que sus características exigen.

Tener presente lo expuesto SERÁ JUSTICIA.

Línea de tiempo de las filtraciones de datos de la Policía Federal Argentina (**#LaGorraLeaks**)

2017

CFP 1033/2017

1 Alguien accede a la cuenta de email de Inteligencia contra el Crimen Organizado de la Policía Federal y envía archivos al periodista Julio López, a Javier Smaldone y a otros.

4 de mayo de 2017 [S]

5 de mayo de 2017

2 Javier Smaldone aporta ante el juez Sebastián Ramos los archivos de la Policía Federal recibidos.

3 El juez Sebastián Ramos ordena al comisario Néstor Roncaglia actualizar **todos los servidores** de la Policía Federal.

9 de mayo de 2017

16 de mayo de 2017

4 Javier Smaldone presta declaración testimonial ante el juez Sebastián Ramos.

En más de **4 años** no se actualizó el servidor de la Superintendencia de Bienestar, a pesar de la orden del juez Sebastián Ramos.

2018

2019

CCC 55276/2019

5 Alguien vulnera el servidor de la Superintendencia de Bienestar. Según la Policía Federal tenía en ese momento PHP 5.6.3 (obsoleto desde **diciembre de 2014**).

28 de julio de 2019 [S]

30 de julio de 2019

6 La Policía Federal denuncia el acceso ilegítimo a 3 cuentas de email. No menciona la vulneración del servidor de la Superintendencia de Bienestar.

21

En **14 días** no hubo avances en la investigación.

7 Alguien publica la filtración #LaGorraLeaks 2.0 con información de la Superintendencia de Bienestar.

12 de agosto de 2019 [S]

8

Javier Smaldone
@mis2centavos

¿Por qué aparece la filtración de 700 Gb de datos de #LaGorraLeaks? Porque durante 2 años, @PatoBullrich y la @PFAOficial no hicieron NADA. Abro hilo. 👇

8:29 p. m. · 12 ago. 2019 · Twitter Web App

12 de agosto de 2019

13 de agosto de 2019

9 La Policía Federal ratifica la denuncia del **30 de julio de 2019**. No menciona la vulneración del servidor de la Superintendencia de Bienestar.

10 La Policía Federal forma un Comité de Seguridad de la Información.

14 de agosto de 2019

15 de agosto de 2019

11 La Policía Federal sindica como uno de los sospechosos a Javier Smaldone.

En **2 días** se señalan sospechosos.

Durante **3 meses** no se reconoció la vulneración del servidor de la Suptcia. de Bienestar.

12 La Policía Federal allana **15 domicilios**, entre ellos el de Javier Smaldone.

8 de octubre de 2019

13 El juez Luis Rodríguez aparta a la Policía Federal de la investigación.

10 de octubre de 2019

29 de octubre de 2019

14 La Policía Federal reconoce la vulneración del servidor de la Superintendencia de Bienestar.

15 El juez Luis Rodríguez delega la instrucción en la Fiscalía 1 (fiscal Jorge Di Lello), para dar intervención a la Unidad Fiscal Especializada en Ciberdelincuencia (fiscal Horacio Azzolin).

18 de diciembre de 2019

20 de diciembre de 2019

16 El fiscal Jorge Di Lello solicita colaboración al fiscal Horacio Azzolin (UFECI).

Nunca se peritó **ninguno** de los dispositivos informáticos secuestrados en los **15 allanamientos** realizados.

2020

La investigación no tuvo **ningún** avance.

2021

17 El fiscal Ramiro González reemplaza al fiscal Jorge Di Lello.

12 de febrero de 2021

22 de marzo de 2021

18 El fiscal Horacio Azzolin emite su dictamen, desvinculando a **algunos** investigados y proponiendo múltiples medidas de prueba.

En casi **8 meses** no se impulsó **ninguna** de las medidas de prueba propuestas por el fiscal Azzolin.

20 El juez Luis Rodríguez sobresee a **todos** los investigados y archiva las actuaciones.

24 de noviembre de 2021

17 de noviembre de 2021

19 El fiscal Ramiro González solicita sobreseer a **todos** los investigados y archivar las actuaciones.

Referencias

1 **2** **4** Fs. 1162-1164.

3 Anexo del escrito presentado por E. V. C. el 08 de abril de 2021.

5 Fs. 1705 vta.

6 Fs. 17.

7 Fs. 28.

8 Fs. 1165.
https://twitter.com/mis2centavos/status/1161057262321983488

9 Fs. 31-32.

10 Sumario N° 465-18-001840/2019 de la Policía Federal, fs. 75.

11 Fs. 67-68.

12 Fs. 735-736.

13 Fs. 642.

14 IF-2019-97174612-APN-SFTIYC#PFA

15 Fs. 1585.

16 Fs. 1618.

17 CUDAP: EXP-MPF 323/2021.

18 Fs. 1681-1692.

19 Dictamen de la Fiscalía Federal N.° 1 del 17 de noviembre de 2021.

20 Resolución del Juzgado Federal N.° 9 del 24 de noviembre de 2021.

21 Fs. 1683.